DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY REFER TO: Joint Interoperability Test Command (JTD) **10 Jul 14**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the McAfee Nitro Intrusion Protection System (IPS), Software Release 9.3.2

References: (a) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(b) DoD CIO, Memorandum, "Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS)," 27 March 2012
(c) through (f), see Enclosure 1

1. **Certification Authority.** References (a) and (b) establish the Joint Interoperability Test Command (JITC) as the Joint Interoperability Certification Authority for the Unified Capabilities (UC) products.

2. **Conditions of Certification.** The McAfee Nitro Intrusion Protection System (IPS), Software Release 9.3.2; hereinafter referred to as the System Under Test (SUT), meets the requirements of the Unified Capabilities Requirements (UCR) 2013, Reference (c), and is certified for joint use as an Intrusion Detection System (IDS)/IPS without any conditions (See Table 1). This certification expires upon changes that affect interoperability, but no later than three years from the date of this memorandum.

Table 1. Conditions

Condition	Operational Impact	Remarks
UCR Waivers		
None	None	None
Conditions of Fielding		
None	None	None
Open Test Discrepancies		
None	None	None

LEGEND:

UCR Unified Capabilities Requirements

3. **Interoperability Status.** Table 2 provides the SUT interface interoperability status and Table 3 provides the Capability Requirements (CR) and Functional Requirements (FR) status. Table 4 provides a UC Approved Products List (APL) product summary.

Table 2. Interface Status

Interface (See Note 1.)	Threshold CR/FR Requirements (See note 2.)	Status	Remarks
Security Devices			
10Base-X	1-3	Met	None
100Base-X	1-3	Met	None
1000Base-X	1-3	Met	None
10GBase-X	1-3	Met	None
40GBase-X	1-3	N/A	None
100GBase-X	1-3	N/A	None

NOTES:
1. UCR 2013, Section 13 does not identify individual interface requirements for security devices. The SUT must minimally provide Ethernet interfaces that meet the requirements in Section 2.7.1.
2. The CR/FR requirements are contained in Table 2. The CR/FR numbers represent a roll-up of UCR 2013 requirements. Enclosure 3 provides a list of more detailed requirements for security devices.

LEGEND:

Base-X	Ethernet generic designation (Baseband)	N/A	Not Applicable
CR	Capability Requirements	SUT	System Under Test
FR	Functional Requirements	UCR	Unified Capabilities Requirements
GBase-X	Gigabit generic designation (Baseband)		

Table 3. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	UCR Requirement (High-Level) (See note 1.)	UCR 2013 Reference	Status
1	Information Assurance (see note 2)	4	Met
2	IPv6	5	Met
3	Security Device Requirements	13.2	Met

NOTES:
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3; Table 3-2 provides detailed CR/FR for security devices.
2. Security testing is accomplished by Joint Interoperability Test Command Indian Head-led Information Assurance test teams and the results published in a separate report, Reference (e).

LEGEND:

CR	Capability Requirements	IPv6	Internet Protocol version 6
FR	Functional Requirements	SUT	System Under Test
ID	Identification	UCR	Unified Capabilities Requirements

Table 4. UC APL Product Summary

Product Identification	
Product Name	McAfee Nitro Intrusion Protection System (IPS)
Software Release	Software Release 9.3.2
UC Product Type(s)	Intrusion Detection System/IPS
Product Description	The McAfee Nitro IPS solution provides network monitoring capabilities allowing an administrator to watch the network for anomalies that might be indicative of a network intrusion; recording evidence of the penetration and/or actively disrupting the attack.

Table 4. UC APL Product Summary (continued)

Product Components	Component Name	Versions	Remarks
An intelligent packet-filtering system that detects sophisticated network intrusion attempts and actively records and/or thwarts such attempts.	Intrusion Protection System	McAfee SIEM 9.3.2	NTP26004BTX
Command center for all devices under its scope.	Enterprise Security Manager	McAfee SIEM 9.3.2	ELU
Passively monitors traffic captured using the Nitro IPS driver.	Application Data Monitor	McAfee SIEM 9.3.2	APM3450
Database auditing solution, automates the collection, management, analysis, and visualization/reporting of database access for virtually all popular database platforms.	Database Event Monitor	McAfee SIEM 9.3.2	DSM2600

NOTES:
1. The detailed component and subcomponent list is provided in Enclosure 3.

LEGEND:

APL	Approved Products List	IPS	Intrusion Protection System
APM	Application Data Monitor	SIEM	Security Information and Event Manager
ELU	Enterprise Log Manager and Even Receiver	UC	Unified Capabilities

4. **Test Details.** This certification is based on interoperability testing, Defense Information Systems Agency (DISA) adjudication of open Test Discrepancy Reports (TDRs), review of the vendor's Letters of Compliance (LoC), and DISA Certifying Authority (CA) Recommendation for inclusion on the UC APL. Testing was conducted at the JITC Information Assurance (IA) Lab at Indian Head, Maryland, 20 through 31 January 2014 using test procedures derived from Reference (d). DISA adjudication of outstanding TDRs completed 01 April 2014. Review of the vendor's LoC completed 21 January 2014. The DISA CA provided a positive recommendation on 05 June 2014 based on the security testing completed by JITC Indian Head-led IA test teams and the results published in a separate report, Reference (e). Enclosure 2 documents the test results and describes the tested network and system configurations. Enclosure 3 provides a detailed list of the interface, capability, and functional requirements.

5. **Additional Information.** JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. Interoperability status information is available via the JITC System Tracking Program (STP). STP is accessible by .mil/.gov users at https://stp.fhu.disa.mil/. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at https://jit.fhu.disa.mil/. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly from the Unified Capabilities Certification Office (UCCO) by government civilian or uniformed military personnel e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil. All associated information is available on the DISA UCCO website located at http://www.disa.mil/Services/Network-Services/UCCO.

6. **Point of Contact (POC).** The JITC testing point of contact is Mr. Keith Watson; commercial (301) 743- 4305; e-mail address is keith.d.watson2.civ@mail.mil. The JITC certification point

of contact is Ms. Jaime Downing, commercial telephone (301) 743-4306; e-mail address is Jaime.f.downing.civ@mail.mil; mailing address Joint Interoperability Test Command, ATTN: JTD (Ms. Jaime Downing) 3341 Strauss Ave., Suite 236, Indian Head, MD 20646-5149. The UCCO tracking number for the SUT is 1308803.

FOR THE COMMANDER:

Adam K. Britt

3 Enclosures a/s

for RIC J. HARRISON
Chief
Networks/Communications and UC Portfolio

Distribution (electronic mail):
DoD CIO
Joint Staff J-6, JCS
USD (AT&L)
ISG Secretariat, DISA, JTA
US Strategic Command, J665
US Navy, OPNAV N2/N6FP12
US Army, DA-OSA, CIO/G-6 ASA (ALT), SAIS-IOQ
US Air Force, A3CNN/A6CNN
US Marine Corps, MARCORSYSCOM, SIAT, A&CE Division
US Coast Guard, CG-64
DISA/TEMC
DIA, Office of the Acquisition Executive
NSG Interoperability Assessment Team
DOT&E, Netcentric Systems and Naval Warfare
Medical Health Systems, JMIS IV&V
HQUSAISEC, AMSEL-IE-IS
UCCO

ADDITIONAL REFERENCES

(c) Office of the Department of Defense Chief Information Officer, "Department of Defense Unified Capabilities Requirements 2013 Errata-1," July 2013
(d) Joint Interoperability Test Command, "Security Device Test Plan"
(e) Joint Interoperability Test Command, "Information Assurance (IA) Assessment Report for McAfee Nitro Intrusion Protection System (IPS) Software Release 9.3.2."
(f) McAfee Internet Protocol version 6 Letter of Compliance for McAfee Nitro IPS v9.1.3, March 2013

(This page intentionally left blank.)

CERTIFICATION SUMMARY

1. SYSTEM AND REQUIREMENTS IDENTIFICATION. The McAfee Nitro Intrusion Protection System (IPS), Software Release 9.3.2 is hereinafter referred to as the Systems Under Test (SUT). Table 2-1 depicts the SUT System and Requirements Identification.

Table 2-1. System and Requirements Identification

System Identification	
Sponsor	United States Army
Sponsor Point of Contact	Mr. Willie Arrington, United States Army, e-mail: willie.l.arrington.civ@mail.mil, telephone number: (210) 722-3463. Mr. Mahesh Shah, United States Army, e-mail: mahesh.s.shah.civ@mail.mil, telephone number: (443) 395-2009.
Vendor Point of Contact	Andrew Nissan, 651-628-5385, email: andy_nissen@mcafee.com
System Name(s)	McAfee Nitro Intrusion Protection System
Increment and/or Version	Software Release 9.3.2
Product Category	Unified Capabilities (UC) Security Devices
System Background	
Previous certifications	None
Tracking	
UCCO ID	1308803
System Tracking Program ID	
Requirements Source	
Unified Capabilities Requirements	Unified Capabilities Requirements 2013 Errata-1 July 2013
Remarks	
Test Organization(s)	JITC

LEGEND:

JITC	Joint Interoperability Test Command	UC	Unified Capabilities
ID	Identification	UCCO	Unified Capabilities Certification Office

2. SYSTEM DESCRIPTION.

Intrusion Prevention System (**IPS**), also known as intrusion detection and prevention system, is a network security appliance that monitor network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it. IPS is considered an extension of Intrusion Detection System (IDS) because they both monitor network traffic and/or system activities for malicious activity. The main differences is, unlike IDS, IPS is placed in-line and able to actively prevent/block intrusions that are detected. More specifically, IPS can take such actions as sending an alarm, dropping the malicious packets, resetting the connection and/or blocking the traffic from the offending Internet Protocol (IP) address. An IPS can also correct Cyclic Redundancy Check errors, unfragment packet streams, prevent Transport Control Protocol (TCP) sequencing issues, and clean up unwanted transport and network layer options.

TN1308803 – McAfee Nitro Intrusion Protection System

The McAfee Nitro IPS solution provides network monitoring capabilities allowing an administrator to watch the network for anomalies that might be indicative of a network intrusion; recording evidence of the penetration and/or actively disrupting the attack. The solution can be configured to selectively pass, drop, or log packets as they arrive based on a user-defined rule set. Configuration is maintained by a central management device which also has the ability to provide for the management, reporting, and analysis of event and flow data gathered from the network.

The Enterprise Security Manager (ESM) acts as the command center for all devices. The ESM 9.3.2 is delivered as software installed on a VMware ESXi 5.0 Server. The management method includes accessing the application via Hypertext Transfer Protocol Secure (HTTPS) for a secure encrypted session tunneling via Public Key Infrastructure/Common Access Card (PKI/CAC) enabled workstation. Access is authenticated using certificate credentials obtained from a CAC, which maps to the associated McAfee user account.

Nitro IPS. The Nitro IPS device is an intelligent packet-filtering system that detects sophisticated network intrusion attempts and actively records and/or thwarts such attempts. The device incorporates a high-performance embedded data manager that is used for administration, data acquisition analysis, and advanced intrusion analytics such as anomaly detection.

The device selectively passes, drops, and logs packets as they arrive, based on a user-defined rule set that is specified by an industry-standard rule language. Additionally, each Nitro IPS contains a fully functional firewall component controlled by industry-standard firewall rules providing low-level packet inspection capabilities and an industry-standard system log. Nitro IPS is managed via a secure connection from an ESM device.

ESM, Enterprise Log Manager, and Event Receiver. These devices act as the command center for all devices under its scope and the following major functions:

- Device configuration for both the Nitro IPS and its embedded firewall component.
- Management, reporting, and analysis of event and flow data gathered from a Nitro IPS device.
- Notification and logging based on user-specified conditions.
- Retrieval of new signatures and software updates.
- Tracking of device activity and status.

The database is not open to users but embedded within the application.

Application Data Monitor (APM). The APM passively monitors traffic captured using the Nitro IPS driver. It monitors, decodes, and detects anomalies in the following application protocols:

- File Transfer: File Transfer Protocol, Hypertext Transfer Protocol, System Specific Language (setup/certificates only)

- Email: Simple Mail Transfer Protocol, Post Office Protocol version 3, Network News Transfer Protocol, Messaging Application Programming Interface
- Chat: Microsoft Network, America Online, Inc (AOL) Instant Messenger/Oscar, Yahoo, Jabber, Internet Relay Chat
- Web Mail: Hotmail, Hotmail DeltaSync, Yahoo mail, AOL, Google Mail, Google Mail
- P2P: Gnutella, bitTorrent
- Shell: Secure Shell (detection only), Telnet

The APM accepts rule expressions and tests them against monitored traffic, inserting records into the event table of the database for each triggered rule. It stores the packet that triggered the rule in the event table's packet field. In addition, it adds application level metadata to the database session and query tables of the database for every triggered rule. It stores a text representation of the protocol stack in the query table's packet field. The APM is managed via a secure connection from an ESM device.

Database Event Monitor (DSM). The DSM is McAfee's award-winning database auditing solution, automates the collection, management, analysis, and visualization/reporting of database access for virtually all popular database platforms. It delivers a comprehensive, detailed security auditing solution for web and database applications vulnerable to insider theft and application-layer attacks. The McAfee DSM is available as preconfigured hardened Linux appliances and includes preconfigured rules and reports for common business problems including Sarbanes-Oxley, Health Insurance Portability and Accountability Act of 1996, Payment Card Industry, Federal Information Security Management Act of 2002, and others.

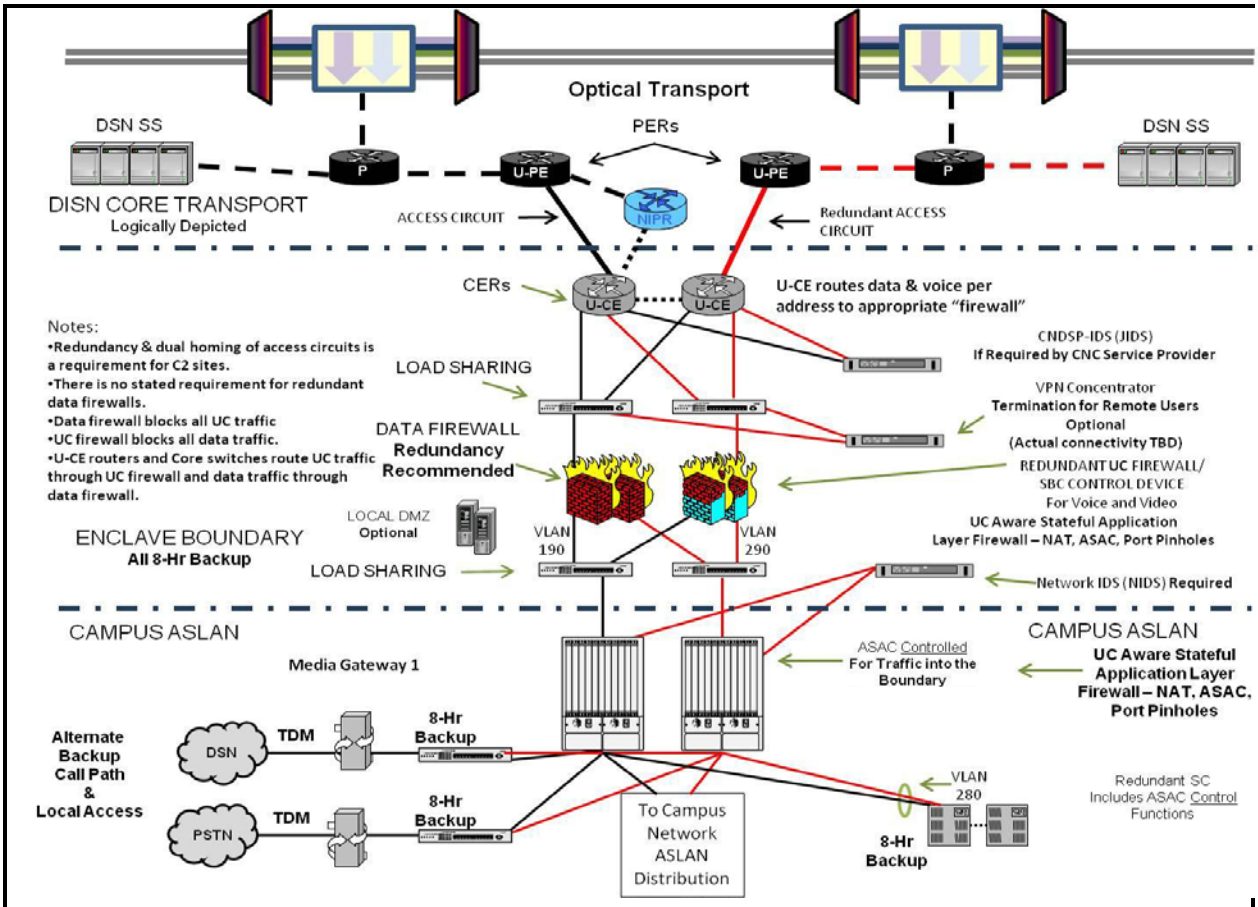
Additionally, McAfee DSM provides continuous, real-time audit trails of all database activity by analyzing the underlying database application protocols. It can monitor logins, logouts, and failed login attempts, alert on unauthorized access from particular logins or client computers, and alert on access to specific objects. It can also capture data changes originated by users and track administrator-initiated access control or schema changes. It even provides a complete audit trail of all requests that can be replayed in a controlled environment. The DSM is managed via a secure connection from an ESM device.

3. OPERATIONAL ARCHITECTURE. The Unified Capabilities (UC) architecture is a two-level network hierarchy consisting of Defense Information Systems Network (DISN) backbone switches and Service/Agency installation switches. The Department of Defense (DoD) Chief Information Officer (CIO) and Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The UC architecture, therefore, consists of several categories of switches. Figure 2-1 depicts the Notional UC Network Architecture and Figure 2-2 depicts the UC Security Device Functional Reference Model.

4. TEST CONFIGURATION. The test team tested the SUT at Joint Interoperability Test Command (JITC), Information Assurance (IA) Laboratory, Indian Head, Maryland, in a manner and configuration similar to that of a notional operational environment. Testing of the system's required functions and features was conducted using the test configuration depicted in Figure

2-3. Interoperability Testing was conducted after IA testing using the same configuration.

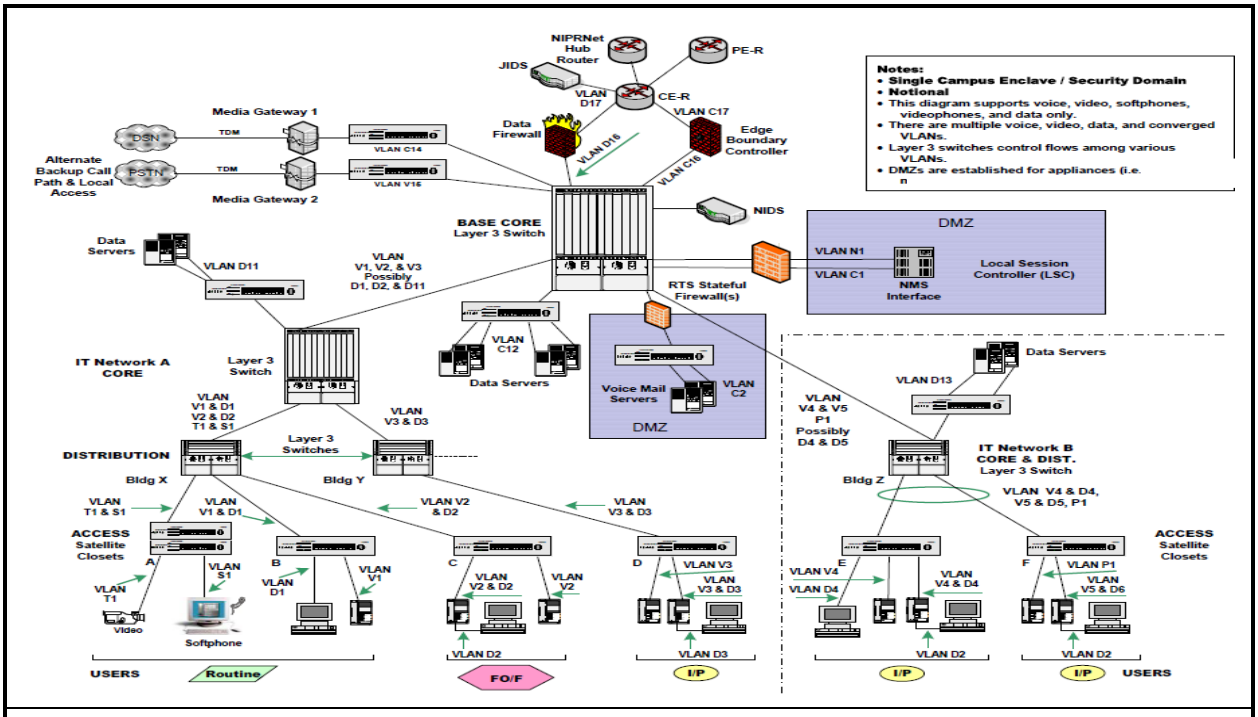
5. METHODOLOGY. Testing was conducted using UC Security Device (SD) requirements derived from the Unified Capabilities Requirements (UCR) 2013 Errata-1, Reference (c), and UC Security Device Test Plan, Reference (d). Any discrepancy noted in the operational environment will be evaluated for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of DISA via a vendor Plan of Action and Milestones (POA&M), which will address all new critical Test Discrepancy Reports (TDRs) within 120 days of identification.



LEGEND:

ASAC	Assured Services Admission Control	P	Premise
ASLAN	Assured Services Local Area Network	PER	Premise Edge Router
C2	Command & Control	PSTN	Public Switched Telephone Network
CER	Customer Edge Router	SBC	Session Border Controller
CNC	Customer Network Controller	SC	Section Controller
CNDSP	Computer Network Defense Service Provider	SS	Softswitch
DSN	Defense Switch Network	TBD	To Be Determined
DISN	Defense Information Systems Network	TDM	Time Division Multiplexing
DMZ	Demilitarized Zone	U-CE	Unclassified – Customer Edge
IDS	Intrusion Detection System	U-PE	Unclassified – Premise Edge
JIDS	Joint Intrusion Detection System	UC	Unified Capabilities
NAT	Network Address Translation	VPN	Virtual Private Network
NIDS	Network Intrusion Detection System	VLAN	Virtual Local Area Network
NIPR	Unclassified-But-Sensitive Internet Protocol Router		

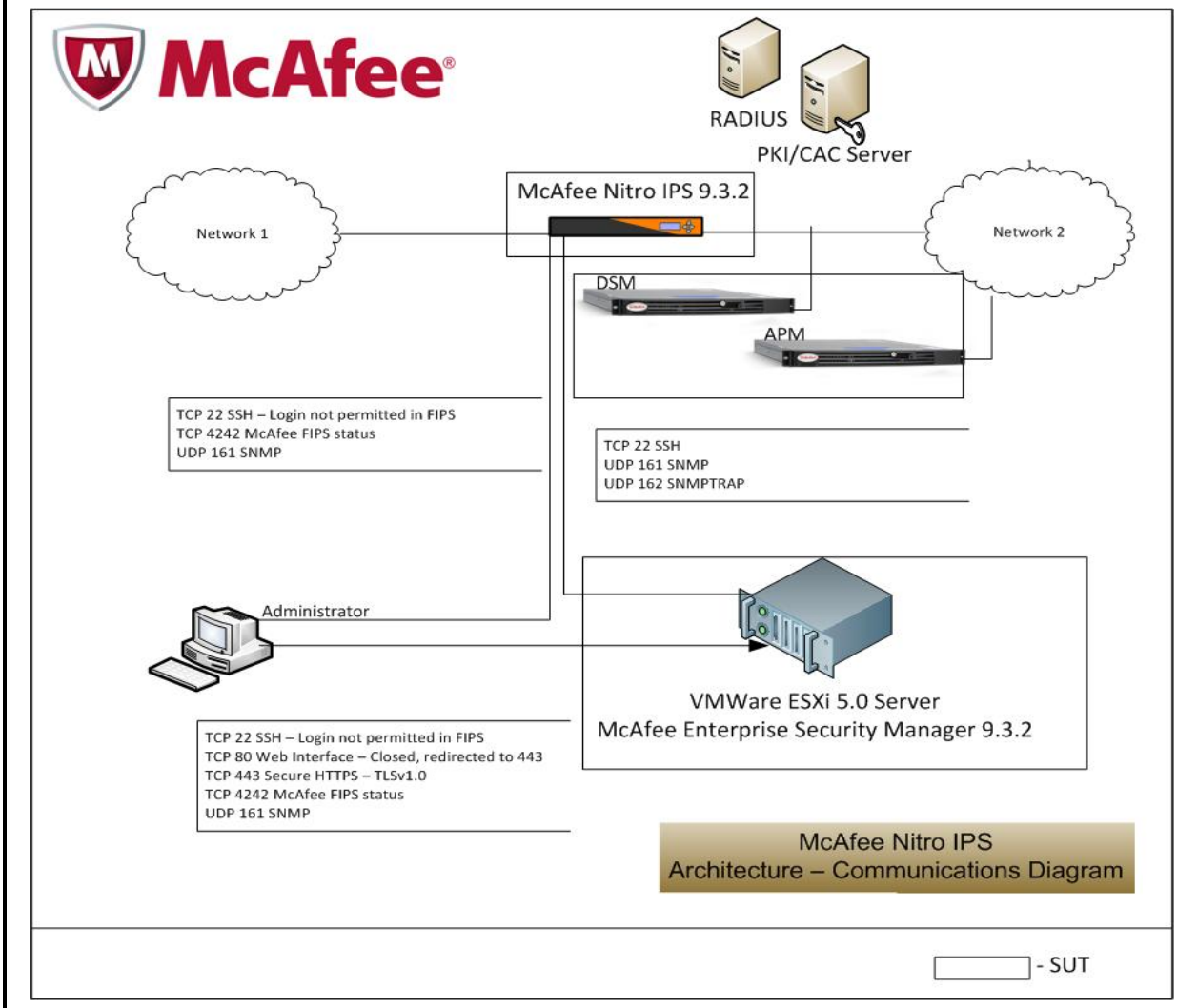
Figure 2-1. Notional UC Network Architecture



LEGEND:

Bldg	Building
CE-R	Core Edge Router
Dist	Distribution
DMZ	Demilitarized Zone
DSN	Defense Switched Network
I/P	Internet Protocol
IT	Information Technology
JIDS	Joint Intrusion Detection System
LSC	Local Session Controller
NID	Network Intrusion Detection System
NIPRNet	Unclassified-But-Sensitive Internet Protocol Router Network
NMS	Network Management System
PE-R	Perimeter Edge Router
PSTN	Public Switched Telephone Network
RTS	Real Time Services
SUT	System Under Test
TDM	Time Division Multiplexing
VLAN	Virtual Local Area Network

Figure 2-2. UC Security Device Functional Reference Model



LEGEND:

APM	Application Data Monitor	RADIUS	Remote Authentication Dial In User Service
CAC	Common Access Card	SNMP	Simple Network Management Protocol
DSM	Database Event Monitor	SSH	Secure Shell
FIPS	Federal Information Processing Standards	SUT	System Under Test
HTTPS	Hypertext Transport Protocol Serve – Secure	TCP	Transport Control Protocol
IPS	Intrusion Protection System	TLS	Transport Layer Security
PKI	Public Key Infrastructure	UDP	User Datagram Protocol

Figure 2-3. SUT Test Configuration

6. INTEROPERABILITY REQUIREMENTS, RESULTS, AND ANALYSIS. The interface, Capability Requirements (CR) and Functional Requirements (FR), IA, Internet Protocol version 6 (IPv6), and Requirements for security devices (SD) are established by UCR 2013, sections 4, 5, and 13. Please refer to Table 3-5 for a detailed list of requirements.

a. Interface Requirements

Security Devices. Table 3-1 provides the SUT interfaces tested.

b. Capability and Functional Requirements. Table 3-2 provides the SUT CRs and FRs tested.

(1) IA Requirements. This section defines the interoperability focused IA requirements for UC products. This section of the UCR also incorporates the general information assurance requirements for a number of UC APL "Security Devices" generally considered to be "Information Assurance Products" in accordance with DoD Directive (DoDD) 8500.1.

(a) Section 4.2.3 of UCR 2013 provided the interoperability focused IA requirements for user roles. The product needs to support at least four roles: Cryptographic Administrator, Audit Administrator, System Administrator, and User.

- The SUT met the minimum requirements through the vendor SD Letter of Compliance (LoC) and testing as an IPS.

(b) Section 4.2.4 of UCR 2013 provided the IA requirements for ancillary equipment such as RADIUS, TACACS+, DHCP, etc.

- The SUT met the minimum requirements through the vendor SD LoC and testing as an IPS.

(c) Section 4.2.7 of UCR 2013 provided the IA requirements for Public Key Infrastructure.

- The SUT met the minimum requirements through the vendor SD LoC and testing as an IPS.

(d) Section 4.2.8 of UCR 2013 provided the IA requirements for integrity such as the product is capable of using Transport Layer Security for providing integrity of AS-SIP messages, provides data integrity of the Secure Real-Time Transport Protocol (SRTP) bearer (transport) packets, etc.

- The SUT met the minimum requirements through the vendor SD LoC and testing as an IPS.

(e) Section 4.2.9 of UCR 2013 provided the IA requirements for confidentiality.

- The SUT met the minimum requirements through the vendor SD LoC and testing as an IPS.

(f) Section 4.2.10 of UCR 2013 provided the IA requirements for non-repudiation.

- The SUT met the minimum requirements through the vendor SD LoC and testing as an IPS.

(2) Internet Protocol version 6 (IPv6) Requirements

(a) Section 5.2.1 of UCR 2013 provided the detailed IPv6 product requirements for SD: Maximum Transmission Unit, Flow Label, Address, Neighbor Discovery, Stateless Address Autoconfiguration and Manual Address Assignment, Internet Control Message Protocol, Traffic Engineering, IP Version Negotiation.

- The SUT met the minimum requirements through the vendor SD LoC as an IPS.

(b) Section 5.2.2 of UCR 2013 provided the detailed Mapping of RFCs to UC Profile Categories product requirements for security devices.

- The SUT met the minimum requirements through the vendor SD LoC and testing as an IPS.

(3) Security Device Requirements

(a) Conformance. Section 13.2.1 of UCR 2013 provided the conformance requirements for VPN.

- This section is N/A for IPS.

(b) General. Section 13.2.2 of UCR 2013 provided the general requirements for FW, IPS, VPN, NAC, and WIDS.

- The SUT met the minimum requirements through the vendor SD LoC and testing as an IPS.

(c) Performance. Section 13.2.3 of UCR 2013 provided the performance requirements for FW, IPS, VPN, and WIDS. Security devices are intended to mitigate the threats enclaves face from external sources while permitting transmission of legitimate traffic in both directions. Performance tests attempt to validate a security device's ability to maintain that legitimate traffic stream while the network is under attack.

- The SUT met the minimum requirements through the vendor SD LoC and testing as an IPS.

(d) Functionality**.** In addition to Section 4, the UCR 2013 Section 13.2.4 also specifies functional requirements for "security-device-unique" products such as network-based Firewalls (FWs), Intrusion Prevention Systems (IPSs), Virtual Private Network (VPN) concentrators, Integrated Security System (ISSs), Wireless Intrusion Detection Systems (WIDS), and Network Access Controllers (NAC).

1. Section 13.2.4.1.1 of UCR 2013 provided policy requirements for DFW and VPN. This section identifies the need for a security device to respond to policy-based actions set by a System Administrator.

- This section is N/A for IPS.

2. Section 13.2.4.1.2 of UCR 2013 provided filtering requirements for DFW to perform basic filtering functions. The security device's controlled interface must support and filter communications protocols/services from outside the perimeter of the interconnected ISs according to IS-appropriate needs (e.g., filter based on addresses, identity, protocol, authenticated traffic, and applications). Filtering is defined as having the ability to block on a per-interface basis, defaulting to block, and defaulting to disabled, if supported on the security device itself.

- This section is N/A for IPS.

3. Section 13.2.4.2 of UCR 2013 provided functionality requirements for IPS and WIDS.

- The SUT met the minimum requirements through the vendor SD LoC and testing as an IPS

4. Section 13.2.4.2.1 of UCR 2013 is for any IPS device that has the capability to inspect VVoIP signals correctly.

- This section is N/A.

(4) Integrated Security Systems Requirements. Section 13.2.4.3 of UCR 2013 listed requirements for Integrated Security Systems (ISSs) systems that provide the functionality of more than one Information Assurance device in one integrate device.

- This section is N/A for IPS.

(5) Information Assurance Tools Requirements. Section 13.2.4.4 of UCR 2013 provided requirements for Information Assurance Tools (IATs). IAT is a category of Information Assurance devices that are not yet fully defined. These devices must meet the Information Assurance requirements for DoD systems as defined in UCR 2013 Section 4, Information Assurance. Functional requirements will be added in future versions of UCR document.

- This section is N/A for IPS.

(6) Network Access Controllers Requirements. Section 13.2.4.5 of UCR 2013 provided requirements for Network Access Controller (NAC). NAC attempt to control access to a network with policies including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do. A system is composed of many elements and is not a single device.

- This section is N/A for IPS.

Table 3-3 provides the SUT components' hardware, software, and firmware tested. JITC Indian Head tested the SUT in an operationally realistic environment to determine its interoperability capability with associated network devices and network traffic. Table 3-4 provides the hardware, software, and firmware of the components used in the test infrastructure.

7. TESTING LIMITATIONS. The JITC IA Lab Indian Head, MD test teams noted there are no testing limitations or untested requirements.

8. CONCLUSION(S). The SUT meets the critical interoperability requirements for a UC Security Device as an IPS in accordance with the UCR 2013 and is/are certified for joint use with other UC Products listed on the Approved Products List (APL) with the conditions described in Table 1. The SUT meets the interoperability requirements for the interfaces listed in Table 3-1 and Security Device Capability/Functional Requirements listed in Table 3-5.

DATA TABLES

Table 3-1. Interface Status

Interface (See Note 1.)	Critical	Threshold CR/FR Requirements (See note 2.)	Status	Remarks
Security Device All SUT				
10Base-X	No	1-3	Met	
100Base-X	No	1-3	Met	
1000Base-X	No	1-3	Met	
10GBase-X	No	1-3	Met	
40GBase-X	No	1-3	N/A	
100GBase-X	No	1-3	N/A	

NOTES:
1. UCR 2013, Section 13 does not identify individual interface requirements for security devices. The SUT must minimally provide Ethernet interfaces that meet the requirements in Section 2.7.1.
2. The CR/FR requirements are contained in Table 3. The CR/FR numbers represent a roll-up of UCR 2013 requirements. Enclosure 3 provides a list of more detailed requirements for security devices.

LEGEND:

Base-X	Ethernet generic designation	N/A	Not Applicable
CR	Capability Requirements	SUT	System Under Test
FR	Functional Requirements	UCR	Unified Capabilities Requirements
GBase-X	Gigabit generic designation		

Table 3-2. Capability and Functional Requirements and Status

CR/FR ID	Capability/ Function	Applicability (See Note 1.)	UCR 2013 Reference	Status	Remarks
1	**Information Assurance (IA) Requirements**				
	User Roles	Required	4.2.3	Met	
	Ancillary Equipment	Required	4.2.4	Met	
	Public Key Infrastructure	Required	4.2.7	Met	
	Integrity	Required	4.2.8	Met	
	Confidentiality	Required	4.2.9	Met	
	Non-Repudiation	Required	4.2.10	Met	
2	**Internet Protocol Version 6 (IPv6) Requirements**				
	Product Requirements	Required	5.2.1	Met	
	Mapping of RFCs to UC Profile Categories	Required	5.2.2	Met	
3	**Security Device Requirements**				
3-1	Conformance	Required	13.2.1	N/A	
3-2	General	Required	13.2.2	Met	
3-3	Performance	Required	13.2.3	Met	
3-4	**Functionality**				
3-4a	**DFW and VPN**				
	Policy	Required	13.2.4.1.1	N/A	
	Filtering	Required	13.2.4.1.2	N/A	
3-4b	**IPS and WIDS**				
	IPS	Required	13.2.4.2	Met	
	IPS VVoIP Signal and Media Inspection	Optional	13.2.4.2.1	N/A	
3-4c	**Integrated Security Systems (ISS)**				
	ISS	Required	13.2.4.3	N/A	
3-4d	**Information Assurance Tools**				
	IAT	Optional	13.2.4.4	N/A	
3-4e	**Network Access Controllers**				
	NAC	Required	13.2.4.5	N/A	

NOTES:
1. The annotation of 'required' refers to a high-level requirement category. The applicability of each sub-requirement is provided in Enclosure 3; Table 3-1 provides detailed CR/FR for security devices.

LEGEND:

CR	Capability Requirement	N/A	Not Applicable
FR	Functional Requirement	NAC	Network Access Control
DFW	Data Firewall	RFC	Request For Comment
IA	Information Assurance	UC	Unified Capabilities
IAT	Information Assurance Tools	UCR	Unified Capabilities Requirements
ID	Identification	VPN	Virtual Private Network
IPv6	Internet Protocol version 6	VVoIP	Video and Voice over Internet Protocol
IPS	Intrusion Prevention System	WIDS	Wireless Intrusion Detection System
ISS	Integrated Security System		

Table 3-3. SUT Hardware/Software/Firmware Version Identification

Component	Release	Function
NTP26004BTX	9.3.2	An intelligent packet-filtering system that detects sophisticated network intrusion attempts and actively records and/or thwarts such attempts.
ELU	9.3.2	Command center for all devices under its scope.
APM3450	9.3.2	Passively monitors traffic captured using the Nitro IPS driver.
DSM2600	9.3.2	Database auditing solution, automates the collection, management, analysis, and visualization/reporting of database access for virtually all popular database platforms

LEGEND:

APM	Application Data Monitor	RAM	Radom Access Memory
DSM	Database Event Monitor	SSD	Solid State Drive
ELU	Enterprise Security Manager	SUT	System Under Test
GB	Gigabit	TB	Terabyte
HD	Hard drive	U	Units
OS	Operating System		

Table 3-4. Test Infrastructure Hardware/Software/Firmware Version Identification

System Name	Software Release	Function
Required Ancillary Equipment		
Server (HP ProLiant DL380 G8)	RHEL 5	RADIUS / SYSLOG
Server (HP Z600)	Windows 2008R2 DoD Baseline	Active Directory
Test Network Components		
Workstation (HP EliteBook 8770w)	Windows 7 DoD Baseline	Management
Switch (Cisco SG200)	1.0.5.1	LAN Switch
Hub (Kingston KND800TX)	N/A	Hub
Ixia IxLoad	4.00	TGA
Agilent Ixia 400	Version 6.1 Release 1	TGA

LEGEND:

DoD	Department of Defense	RHEL	Red Hat Enterprise Linux
HP	Hewlett Packard	SP1	Service Pack 1
LAN	Local Area Network	SYSLOG	System Log
N/A	Not Applicable	TGA	Traffic Generation Appliance
RADIUS	Remote Authentication Dial - In User Service		

Table 3-5. Security Device Capability/Functional Requirements

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
1	**Information Assurance Requirements**										
1.1	**User Roles**										
1	04.2.3	User Roles	IA-004000	The product shall be capable of providing a mechanism for the appropriate administrator (not a user in the User role) to perform the following functions:	**R**	**R**	**R**	**R**	**R**	**R**	**R**
2	04.2.3	User Roles	IA-004010	Monitor the activities of a specific terminal, port, or network address of the system in real time.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
3	04.2.3	User Roles	IA-004020	Define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
4	04.2.3	User Roles	IA-004030	Provide a capability to monitor the system resources and their availabilities.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
5	04.2.3	User Roles	IA-005000	The product shall support at least four roles: Cryptographic Administrator (CAdmin), Audit Administrator (AAdmin), System Administrator, User. NOTE: The CAdmin and AAdmin roles are defined in NIAP publications.	**R**	**R**	**R**	**R**	**N/A**	**R**	**R**
6	04.2.3	User Roles	IA-006010	Modify security functions.	**R**	**R**	**R**	**R**	**N/A**	**R**	**R**
7	04.2.3	User Roles	IA-006020	Enable or disable security alarm functions.	**R**	**R**	**R**	**R**	**N/A**	**R**	**R**
8	04.2.3	User Roles	IA-006030	Enable or disable the Internet Control Message Protocol (ICMP) and destination unreachable notification on external interfaces (in an IP-based network), or other appropriate network connectivity tool (for a non-IP-based network).	**R**	**R**	**R**	**R**	**N/A**	**R**	**R**
9	04.2.3	User Roles	IA-006040	Determine the administrator-specified period for any policy.	**R**	**R**	**R**	**R**	**N/A**	**R**	**R**
10	04.2.3	User Roles	IA-006050	Set the time/date used for timestamps.	**R**	**R**	**R**	**R**	**N/A**	**R**	**R**
11	04.2.3	User Roles	IA-006060	Query, modify, delete, and/or create the information flow policy rule set.	**R**	**R**	**R**	**R**	**N/A**	**R**	**R**
12	04.2.3	User Roles	IA-006070	Revoke security attributes associated with the users, information flow policy rule set, and services available to unauthenticated users within the VPN, DFW, IPS, ISS, NAC, and IAT.	**R**	**R**	**R**	**R**	**N/A**	**R**	**R**
13	04.2.3	User Roles	IA-007000	The ability to enable, disable, determine, and/or modify the functions of the security audit or the security audit Analysis shall be restricted to the AAdmin role.	**R**	**R**	**R**	**R**	**N/A**	**R**	**R**
14	04.2.3	User Roles	IA-008000	The ability to perform the following functions shall be restricted to the CAdmin role:	**R**	**R**	**R**	**R**	**N/A**	**R**	**R**
15	04.2.3	User Roles	IA-008010	Enable and/or disable the cryptographic functions.	**R**	**R**	**R**	**R**	**N/A**	**R**	**R**
16	04.2.3	User Roles	IA-008020	Modify the cryptographic security data.	**R**	**R**	**R**	**R**	**N/A**	**R**	**R**
1.2	**Ancillary Equipment**										
1	04.2.4	Ancillary Equipment	IA-009000	Products that use external AAA services provided by the Diameter Base Protocol shall do so IAW RFC 3588.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
2	04.2.4	Ancillary Equipment	IA-009010	Systems that act as Diameter agents shall be capable of being configured as proxy agents.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
3	04.2.4	Ancillary Equipment	IA-009020	Systems that act as proxy agents shall maintain session state.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
4	04.2.4	Ancillary Equipment	IA-009030	All Diameter implementations shall ignore answers received that do not match a known Hop-by-Hop Identifier field.	**C**	**C**	**C**	**C**	**C**	**C**	**C**

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
5	04.2.4	Ancillary Equipment	IA-009040	All Diameter implementations shall provide transport of its messages IAW the transport profile described in RFC 3539.	C	C	C	C	C	C	C
6	04.2.4	Ancillary Equipment	IA-009050	Products that use the Extensible Authentication Protocol (EAP) within Diameter shall do so IAW RFC 4072.	C	C	C	C	C	C	C
7	04.2.4	Ancillary Equipment	IA-010000	Products shall support the capability to use the Remote Authentication Dial In User Service (RADIUS) IAW RFC 2865 to provide AAA services. NOTE: Unlike previous UCR revisions where RADIUS was a Conditional requirement, RADIUS is now a capability that is Required when supporting AAA services.	R	R	R	R	R	R	R
8	04.2.4	Ancillary Equipment	IA-010010	Products that use the EAP within RADIUS shall do so IAW RFC 3579.	R	R	R	R	R	R	R
9	04.2.4	Ancillary Equipment	IA-010020	If the products support RADIUS based accounting, the system shall do so IAW RFC 2866.	R	R	R	R	R	R	R
10	04.2.4	Ancillary Equipment	IA-011000	Products that use external AAA services provided by the Terminal Access Controller Access Control System (TACACS+) shall do so IAW the TACACS+ Protocol Specification 1.78 (or later). NOTE: The intent is to use the most current TACACS+ specification.	C	C	C	C	C	C	C
11	04.2.4	Ancillary Equipment	IA-013000	Products that use external AAA services provided by port based network access control mechanisms shall do so IAW IEEE 802.1X-2010 in combination with PEAP and EAP-TLS support, at a minimum, plus any other desired secure EAP types (e.g., EAP-Tunneled Transport Layer Security (TTLS).	C	C	C	C	C	C	C
12	04.2.4	Ancillary Equipment	IA-013010	Products that use external EAP services provided by EAP shall do so IAW RFC 3748 and its RFC extensions.	C	C	C	C	C	C	C
13	04.2.4	Ancillary Equipment	IA-014000	Products that use external syslog services shall support the capability to do so IAW RFC 3164.	C	C	C	C	C	C	C
14	04.2.4	Ancillary Equipment	IA-014010	Products that support syslog over UDP IAW RFC 3164 shall use UDP port 514 for the source port of the sender when using UDP for transport.	C	C	C	C	C	C	C
15	04.2.4	Ancillary Equipment	IA-014020	If the product supports syslog, the product shall support the capability to generate syslog messages that have all the parts of the syslog packet as described in Section 4.1 of RFC 3164.	C	C	C	C	C	C	C
16	04.2.4	Ancillary Equipment	IA-014030	If the originally formed message has a TIMESTAMP in the HEADER part, then it shall support the capability to specify this field's value in the local time of the device within its time zone and support the ability to specify this field's value in Greenwich Mean Time (GMT).	C	C	C	C	C	C	C
17	04.2.4	Ancillary Equipment	IA-014040	If the originally formed message has a HOSTNAME field, then it shall contain the hostname as it knows itself. If it does not have a hostname, then it shall contain its own IP address.	C	C	C	C	C	C	C
18	04.2.4	Ancillary Equipment	IA-014050	If the originally formed message has a TAG value, then it shall be the name of the program or process that generated the message.	C	C	C	C	C	C	C
19	04.2.4	Ancillary Equipment	IA-014060	If products use TCP for the delivery of syslog events, then the system shall support the capability to do so IAW the RAW profile defined in RFC 3195.	C	C	C	N/A	N/A	C	C
20	04.2.4	Ancillary Equipment	IA-016000	If this product implements NTP, then the default version must be maintained version 3 (NTPv3), even if higher versions of NTP are supported.	C	C	C	C	C	C	C
1.3	**Public Key Infrastructure**										

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
1	04.2.7	Public Key Infrastructure	IA-040000	The product shall be capable of generating asymmetric keys whose length is at least 2048 for RSA.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
2	04.2.7	Public Key Infrastructure	IA-041000	The product shall be capable of generating symmetric keys whose length is at least 128 bits.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
3	04.2.7	Public Key Infrastructure	IA-042000	The product shall be capable of storing key pairs and their related certificates.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
4	04.2.7	Public Key Infrastructure	IA-043000	The product shall operate with DoD-approved trust points (e.g., public keys and the associated certificates the relying party deems as reliable and trustworthy, typically root CAs). NOTE: Trust points are further defined in Appendix A of this UCR, Definitions, Abbreviations and Acronyms, and References.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
5	04.2.7	Public Key Infrastructure	IA-044000	The product shall be capable of supporting end entity server and device certificates and populating all certificate fields IAW methods described in the "DoD PKI Functional Interface Specification."	**R**	**R**	**R**	**R**	**R**	**R**	**R**
6	04.2.7	Public Key Infrastructure	IA-045000	The product shall be capable of using the LDAPv3, HTTP, or HTTPS as appropriate when communicating with DoD-approved PKIs.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
7	04.2.7	Public Key Infrastructure	IA-046000	If CRLs are used, the product shall be capable of using either the date and time specified in the next update field in the CRL or using a configurable parameter to define the period associated with updating the CRLs.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
8	04.2.7	Public Key Infrastructure	IA-047000	If CRLs are used, the product shall be capable of obtaining the CRL from the CRL Distribution Point (CDP) extension of the certificate in question. The product shall be able to process HTTP pointers in the CDP field whereas the ability to process HTTPS and LDAP pointers is Objective. NOTE: This requirement does not prevent the product from supporting the ability to use manually configured, local CDPs, which differ from the CDP provided in the certificate.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
9	04.2.7	Public Key Infrastructure	IA-048000	If OCSP is used, the product shall support the capability to use both the Delegated Trust Model (DTM), whereby the OCSP responder's signing certificates are signed by DoD approved PKI CAs, and the OCSP Trusted Responder model, where the OCSP responder uses a self-signed certificate to sign OCSP responses, IAW DoD PKI PMO guidance. NOTE: The OCSP responder's DTM certificate is appended to every OCSP response sent from the DoD PKI OCSP responders. Products should expect these certificates to change regularly (approximately every 30 days). NOTE: RFC 2560 describes both the Trust Responder and Delegated Trust (termed "Authorized Responder" within RFC 2560) models. Though DoD PKI-specific implementation details can only be found in DoD PKI PMO publications.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
10	04.2.7	Public Key Infrastructure	IA-049000	If OCSP is used, the OCSP responder shall be contacted based on the following information:	**C**	**C**	**C**	**C**	**C**	**C**	**C**
11	04.2.7	Public Key Infrastructure	IA-049010	The OCSP responder preconfigured in the application or toolkit; and	**C**	**C**	**C**	**C**	**C**	**C**	**C**
12	04.2.7	Public Key Infrastructure	IA-049020	The OCSP responder location identified in the OCSP field of the Authority Information Access (AIA) extension of the certificate in question.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
13	04.2.7	Public Key Infrastructure	IA-049030	The OCSP responder location identified in the OCSP field of the Authority Information Access (AIA) extension of the certificate in question.	**C**	**C**	**C**	**C**	**C**	**C**	**C**

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
14	04.2.7	Public Key Infrastructure	IA-049040	The product should (not shall) be configurable to provide preferences or a preconfigured OCSP responder based on the Issuer DN.	C	C	C	C	C	C	C
15	04.2.7	Public Key Infrastructure	IA-052000	The product shall support all of the applicable requirements in the latest DoD PKE Application Requirements specification published by the DoD PKI PMO. NOTE: At the time of this UCR's writing, the "DoD Class 3 Public Key Infrastructure Public Key-Enabled Application Requirements" document from July 13, 2000 is the latest version of this document.	R	R	R	R	R	R	R
16	04.2.7	Public Key Infrastructure	IA-053000	Systems that perform any PKI operations (e.g., certificate path processing, certificate validation, digital signature generation, and encryption) must support RSA keys up to 2048 bits with Secure Hash Algorithm (SHA)-1 and SHA-2 digital signatures as dictated by the National Institute of Standards and Technology (NIST) Special Publications (SP) 800-57, SP 800-78, and SP 800-131A and the DoD Certificate Policy.	R	R	R	R	R	R	R
17	04.2.7	Public Key Infrastructure	IA-053010	The product shall support the capability to verify certificates, CRLs, OCSP responses, or any other signed data produced by a DoD approved PKI using RSA in conjunction with the SHA-256 algorithm. NOTE: During the migration to SHA-256, certificate chains may contain a mix of certificates signed using either SHA-1 or SHA-256 within the same chain.	R	R	R	R	R	R	R
18	04.2.7	Public Key Infrastructure	IA-054000	The product shall log when a session is rejected due to a revoked certificate.	R	R	R	R	R	R	R
19	04.2.7	Public Key Infrastructure	IA-055000	The product shall be capable of supporting the development of a certificate path and be able to process the path. NOTE: The path development process produces a sequence of certificates that connect a given end-entity certificate to a trust point. The process terminates when either the path tracks from a trust point to an end entity or a problem occurs that prohibits validation of the path.	R	R	R	R	R	R	R
20	04.2.7	Public Key Infrastructure	IA-055010	The path process shall fail when a problem that prohibits the validation of a path occurs.	R	R	R	R	R	R	R
21	04.2.7	Public Key Infrastructure	IA-056000	The product shall be capable of ensuring that the intended use of the certificate is consistent with the DoD-approved PKI extensions.	R	R	R	R	R	R	R
22	04.2.7	Public Key Infrastructure	IA-056010	The product shall be capable of ensuring that the key usage extension in the end entity certificate is set properly.	R	R	R	R	R	R	R
23	04.2.7	Public Key Infrastructure	IA-056020	The product shall be capable of ensuring that the digital signature bit is set for authentication uses.	R	R	R	R	R	R	R
24	04.2.7	Public Key Infrastructure	IA-056030	The product shall be capable of ensuring that the non-repudiation bit is set for non-repudiation uses.	R	R	R	R	R	R	R
25	04.2.7	Public Key Infrastructure	IA-059000	Periodically, the system shall examine all of the certificates and trust chains associated with ongoing, long-lived, sessions. The system shall terminate any ongoing sessions based on updated revocation/trust information if it is determined that the corresponding certificates have been revoked, are no longer trusted, or are expired. NOTE: The system must not terminate VVoIP sessions simply because of a failure to retrieve the latest CRL or perform an online status check.	R	R	R	R	R	R	R
26	04.2.7	Public Key Infrastructure	IA-059010	If the system supports manual loading of a CRL or CTLs configured by an administrator, the system shall check all ongoing sessions as soon as updates to the internally stored CRL or trust lists occur.	C	C	C	C	C	C	C

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
27	04.2.7	Public Key Infrastructure	IA-059020	If the system supports automated retrieval of a CRL from a CDP, the system shall immediately check the certificates and trust chains associated with all ongoing sessions against the newly retrieved CRL.	C	C	C	C	C	C	C
28	04.2.7	Public Key Infrastructure	IA-059030	If the system supports automated retrieval of a CRL from a CDP, the system shall support the ability to configure the interval in which the CRL is retrieved periodically.	C	C	C	C	C	C	C
29	04.2.7	Public Key Infrastructure	IA-059040	If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), the system shall periodically query the responder to determine if the certificates corresponding to any ongoing sessions have been revoked.	C	C	C	C	C	C	C
30	04.2.7	Public Key Infrastructure	IA-059050	If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), by default, for each session, the device shall query the online status check responder every 24 hours for as long as the session remains active.	C	C	C	C	C	C	C
31	04.2.7	Public Key Infrastructure	IA-059060	If the system supports queries against an online status check responder (an OCSP responder in the case of the DoD PKI), the system shall support the ability to configure the interval at which the system periodically queries the online status check responder.	C	C	C	C	C	C	C
32	04.2.7	Public Key Infrastructure	IA-060000	The system shall be capable of sending an alert when installed certificates corresponding to trust chains, OCSP responder certificates, or any other certificates installed on the device that cannot be renewed in an automated manner, are nearing expiration. NOTE: Since EIs and AEIs are not expected to have direct access to the NMS, the SC, or SS is expected to generate this alert to the NMS on behalf of any subtended EIs or AEIs. However, EIs and AEIs should also alert their users via the EI or AEI user interface when certificates are nearing expiration. NOTE: There is no expectation for vendors to develop a proprietary protocol for this purpose. It is sufficient for an SS, or SC to inspect the certificate of a served EI or AEI during registration time and periodically thereafter for the duration of the signaling session. Some products may also store the certificate associated with their subscribing EIs and AEIs so as to enable this check to be performed even when the EIs and AEIs are offline.	R	R	R	R	R	R	R
33	04.2.7	Public Key Infrastructure	IA-060010	By default, the system shall be capable of sending this alert 60 days before the expiration of the installed credentials, which cannot be renewed automatically. This alert should be repeated periodically on a weekly or biweekly basis by default.	R	R	R	R	R	R	R
1.4				**Integrity**							
1	04.2.8	Integrity	IA-065000	If the product uses IPSec, the product shall be capable of using HMAC-SHA (class value 2) as the default IKE integrity mechanism as defined in Reference Appendix A of RFC 2409 for the definition of 'Class Value 2'.	C	C	C	C	C	C	C
2	04.2.8	Integrity	IA-066000	The entire SNMPv3 message shall be checked for integrity and shall use the HMAC-SHA1-96 with 160 bit key length by default.	R	R	R	R	R	R	R
3	04.2.8	Integrity	IA-067000	If the product uses SSHv2, the product shall use HMAC-SHA1-96 with 160 bit key length for data integrity.	C	C	C	C	C	C	C

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
4	04.2.8	Integrity	IA-068000	If the product uses TLS, the product shall be capable of using TLS (SSL v3.1 or higher) in combination with HMAC-SHA1-160 with 160 bit keys to provide integrity for the session packets.	C	C	C	C	C	C	C
1.5				**Confidentiality**							
1	04.2.9	Confidentiality	IA-071000	If IPSec is used, the product shall be capable of using IKE for IPSec key distribution:	C	C	C	C	C	C	C
2	04.2.9	Confidentiality	IA-071010	The product shall be capable of using IKE version 1.	R	R	R	R	R	R	R
3	04.2.9	Confidentiality	IA-071020	Remove per Errata 1.	N/A	N/A	N/A	N/A	N/A	N/A	N/A
4	04.2.9	Confidentiality	IA-071030	If IPSec is used, the product shall be capable of using the Quick Mode as the default Phase II Security Association mechanism for the IPSec service.	C	C	C	C	C	C	C
5	04.2.9	Confidentiality	IA-071040	If IPSec is used, the product shall be capable of using and interpreting certificate requests for Public-Key Cryptography Standard #7 (PKCS#7) wrapped certificates as a request for the whole path of certificates.	C	C	C	C	C	C	C
6	04.2.9	Confidentiality	IA-071050	If IPSec is used, the product shall be capable of using Main Mode associated with the Diffie-Hellman approach for key generation for the security association negotiation.	C	C	C	C	C	C	C
7	04.2.9	Confidentiality	IA-071060	If the product uses IPSec, the system shall be capable of using AES_128_CBC as the default encryption algorithm. The system shall be capable of supporting 3DES-CBC (class value 5) for backwards compatibility with previous UCR revisions.	C	C	C	N/A	N/A	C	C
8	04.2.9	Confidentiality	IA-071070	If the product uses IPSec, then the system shall be capable of using AES_128_CBC as the default encryption algorithm. The system shall be capable of supporting 3DES-CBC (class value 5) for backwards compatibility with previous UCR revisions.	C	C	C	N/A	N/A	C	C
9	04.2.9	Confidentiality	IA-071080	Remove per Errata 1.	N/A	N/A	N/A	N/A	N/A	N/A	N/A
10	04.2.9	Confidentiality	IA-073000	If the product uses TLS, the product shall do so in a secure manner as defined by the following subtended requirements.	C	C	C	C	C	C	C
11	04.2.9	Confidentiality	IA-073010	If the product uses TLS, the system shall be capable of using TLS_RSA_WITH_AES_128_CBC_SHA as its default cipher suite.	C	C	C	C	C	C	C
12	04.2.9	Confidentiality	IA-073020	If the product uses TLS, the system shall be capable of using a default of no compression.	C	C	C	C	C	C	C
13	04.2.9	Confidentiality	IA-073030	If the product uses TLS, the system shall be capable of exchanging TLS messages in a single exchange or multiple exchanges.	C	C	C	C	C	C	C
14	04.2.9	Confidentiality	IA-073040	If TLS session resumption is used, a timer associated with TLS session resumption shall be configurable and the default shall be 1 hour. NOTE: This requirement is not associated with NM-related sessions.	C	C	C	C	C	C	C
15	04.2.9	Confidentiality	IA-073050	If TLS session resumption is used, the maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/confidentiality/authorization process is 1 hour.	C	C	C	C	C	C	C
16	04.2.9	Confidentiality	IA-073060	If the product supports SSL/TLS renegotiation, the product shall support the capability to disable this feature or the product shall support RFC 5746. NOTE: Supporting RFC 5746 includes providing a configurable option to terminate a TLS session if the peer does not support the "renegotiation_info" extension.	R	R	R	R	R	R	R

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
17	04.2.9	Confidentiality	IA-074000	If the product uses SSH, the system shall do so in a secure manner as defined by the following subtended requirements. NOTE: An EI's remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.	C	C	C	C	C	C	C
18	04.2.9	Confidentiality	IA-074010	If the product uses SSH, the system shall be capable of supporting the RSA 2,048-bit key algorithm and the Diffie-Hellman 2,048 bit key algorithm.	C	C	C	C	C	C	C
19	04.2.9	Confidentiality	IA-074020	If the product uses SSH, a client shall close the session if it receives a request to initiate an SSH session whose version is less than 2.0. NOTE: Closing the session may be either a default behavior or a configurable option. If this is a configurable option, the conditions of fielding should clearly specify that this option must be configured.	C	C	C	C	C	C	C
20	04.2.9	Confidentiality	IA-074030	If the product uses SSH, SSH sessions shall rekey at a minimum every gigabyte of data received or every 60 minutes, whichever comes sooner.	C	C	C	C	C	C	C
21	04.2.9	Confidentiality	IA-074040	If the product uses SSH, SSH sessions shall rekey at a minimum every gigabyte of data transmitted or every 60 minutes, whichever comes sooner.	C	C	C	C	C	C	C
22	04.2.9	Confidentiality	IA-074050	If the product uses SSH, the SSH sessions shall minimally support the following encryption algorithms defined in RFC 4253 and RFC 4344: • AES128-CTR, and • AES128-CBC (for backwards compatibility with older UCR versions).	C	C	C	C	C	C	C
23	04.2.9	Confidentiality	IA-074070	If the product uses SSH, SSH sessions shall use TCP as the underlying protocol.	C	C	C	C	C	C	C
24	04.2.9	Confidentiality	IA-074080	Remove per Errata 1.	N/A	N/A	N/A	N/A	N/A	N/A	N/A
25	04.2.9	Confidentiality	IA-074090	Remove per Errata 1.	N/A	N/A	N/A	N/A	N/A	N/A	N/A
26	04.2.9	Confidentiality	IA-074100	If the product uses SSH, the product shall discard SSH packets that exceed the maximum packet size to avoid DoS attacks or buffer overflow attacks.	C	C	C	C	C	C	C
27	04.2.9	Confidentiality	IA-074110	If the product uses SSH, SSH packets shall use random bytes if packet padding is required.	C	C	C	C	C	C	C
28	04.2.9	Confidentiality	IA-074120	If the product uses SSH, the system shall treat all SSH-encrypted packets sent in one direction as a single data stream. For example, the initialization vectors shall be passed from the end of one packet to the beginning of the next packet.	C	C	C	C	C	C	C
29	04.2.9	Confidentiality	IA-074130	If the product uses SSH, the system shall be capable of setting Diffie-Hellman-Group14-SHA1 as the preferred key exchange mechanism for SSH.	C	C	C	C	C	C	C
30	04.2.9	Confidentiality	IA-075000	If the product uses SSH with X.509v3 certificates and provides an SSH server function, the SSH server shall support the capability to use an X.509v3 certificate provided by a DoD-approved PKI.	C	C	C	C	C	C	C
31	04.2.9	Confidentiality	IA-075010	If the product uses SSH with X.509v3 certificates, the SSH Server function shall support, at a minimum, the "x509v3-ssh-rsa" and "x509v3-rsa2048-sha256" key types as defined in RFC 6187.	C	C	C	C	C	C	C
32	04.2.9	Confidentiality	IA-075020	If the product uses SSH with X.509v3 certificates, the SSH Server function shall support the capability to, in a configurable manner, specify the highest preferred key type advertised during the SSH_MSG_KEXINIT message exchange.	C	C	C	C	C	C	C
33	04.2.9	Confidentiality	IA-075030	If the product uses SSH with X.509v3 certificates, the SSH server function shall support the capability to deny SSH sessions when the session fails to negotiate a configured set of preferred key types.	C	C	C	C	C	C	C

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
34	04.2.9	Confidentiality	IA-076000	If the product uses SSH with X.509v3 certificates, the SSH client shall support the capability to use an X.509v3 certificate provided by a DoD-approved PKI.	C	C	C	C	C	C	C
35	04.2.9	Confidentiality	IA-076010	If the product uses SSH and if the SSH client has a CAC (or equivalent) reader, the SSH client may use the X.509v3 certificate on the user's CAC to establish the encrypted session.	C	C	C	C	C	C	C
36	04.2.9	Confidentiality	IA-076020	If the product uses SSH and if the client has a CAC (or equivalent) reader and also has its own PKI certificate from a DoD-approved PKI, the client may use either its certificate or the certificate on the user's CAC to establish the encrypted sessions.	C	C	C	C	C	C	C
37	04.2.9	Confidentiality	IA-076030	If the product uses SSH with X.509v3 certificates, the SSH client shall support, at a minimum, the "x509v3-ssh-rsa" and "x509v3-rsa2048-sha256" key types as defined in RFC 6187.	C	C	C	C	C	C	C
38	04.2.9	Confidentiality	IA-077000	The product shall be capable of using SNMPv3 for all SNMP sessions. NOTE: If the product is using Version 1 or Version 2 (instead of SNMPv3) with all of the appropriate patches to mitigate the known security vulnerabilities, any findings associated with this requirement may be downgraded. In addition, if the product has developed a migration plan to implement Version 3, any findings associated with this requirement may be further downgraded.	R	R	R	R	R	R	R
39	04.2.9	Confidentiality	IA-077010	The security level for SNMPv3 in the DoD VVoIP environment shall be authentication with privacy – snmpSecurityLevel=authPriv. The product shall set snmpSecurityLevel=authPriv as the default security level used during initial configuration.	R	R	R	R	R	R	R
40	04.2.9	Confidentiality	IA-077020	The SNMPv3 implementation shall be capable of allowing an appropriate administrator to manually configure the snmpEngineID from the operator console. A default unique snmpEngineID may be assigned to avoid unnecessary administrative overhead, but this must be changeable.	R	R	R	R	R	R	R
41	04.2.9	Confidentiality	IA-077030	The security model for SNMPv3 shall be the User-Based Security Model – snmpSecurityModel =3.	R	R	R	R	R	R	R
42	04.2.9	Confidentiality	IA-077040	If the product receives response messages, the product shall conduct a timeliness check on the SNMPv3 message.	C	C	C	C	C	C	C
43	04.2.9	Confidentiality	IA-077050	An SNMPv3 engine shall perform time synchronization using authenticated messages.	R	R	R	R	R	R	R
44	04.2.9	Confidentiality	IA-077060	The message processing model shall be SNMPv3 – snmpMessageProcessingModel=3.	R	R	R	R	R	R	R
45	04.2.9	Confidentiality	IA-077070	The product shall support the capability to use CBC-DES (usmDESPrivProtocol) with a 16 octet (128 bit) input key, as specified in RFC 3414, as an encryption cipher for SNMPv3.	R	R	R	R	R	R	R
46	04.2.9	Confidentiality	IA-077080	The product shall support the capability to use the CFB-AES128 encryption cipher usmAesCfb128PrivProtocol for SNMPv3 as defined in RFC 3826 and specify this as the default encryption cipher for SNMPv3.	R	R	R	R	R	R	R
47	04.2.9	Confidentiality	IA-077090	If the product receives SNMPv3 response messages, then the SNMPv3 engine shall discard SNMP response messages that do not correspond to any current outstanding Request messages.	C	C	C	C	C	C	C

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
48	04.2.9	Confidentiality	IA-077100	If the product receives SNMPv3 responses, then the SNMPv3 Command Generator Application shall discard any Response Class PDU for which there is no outstanding Confirmed Class PDU.	C	C	C	C	C	C	C
49	04.2.9	Confidentiality	IA-077110	When using msgID for correlating Response messages to outstanding Request messages, the SNMPv3 engine shall use different msgIDs in all such Request messages that it sends out during a 150 second Time Window.	R	R	R	R	R	R	R
50	04.2.9	Confidentiality	IA-077120	An SNMPv3 Command Generator or Notification Originator Application shall use different request-ids in all Request PDUs that it sends out during a Time Window.	R	R	R	R	R	R	R
51	04.2.9	Confidentiality	IA-077130	When sending state altering messages to a managed authoritative SNMPv3 engine, a Command Generator Application should delay sending successive messages to that managed SNMPv3 engine until a positive acknowledgement is received from the previous message or until the message expires.	R	R	R	R	R	R	R
52	04.2.9	Confidentiality	IA-077140	The product using SNMPv3 shall implement the key-localization mechanism.	R	R	R	R	R	R	R
53	04.2.9	Confidentiality	IA-078000	If the product uses web browsers or web servers, the product web browsers and web servers shall be capable of supporting TLS (SSLv3.1) or higher for confidentiality.	C	C	C	C	C	C	C
54	04.2.9	Confidentiality	IA-079000	The product shall be capable of using SSHv2 or TLS 1.0 (SSLv3.1) or higher for remote configuration of appliances. NOTE: The EIs and AEIs remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.	R	R	R	R	R	R	R
1.6				**Non-Repudiation**							
1	04.2.10	Non-Repudiation	IA-084000	The security log shall be capable of using a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest).	R	R	R	R	R	R	R
2	04.2.10	Non-Repudiation	IA-085000	Only the System Security Administrator and System Administrator roles shall have the ability to retrieve, print, copy, and upload the security log(s).	R	R	R	R	R	R	R
3	04.2.10	Non-Repudiation	IA-086000	The product/system shall be able to generate a human understandable presentation of any audit data stored in the audit trail.	R	R	R	R	R	R	R
4	04.2.10	Non-Repudiation	IA-087000	The product shall locally store (queue) audit log/event data when communication with the management station is unavailable and transmit the queued data when network connectivity is restored. NOTE: In the case of protocols that use unreliable delivery, such as syslog over UDP, use of mechanisms at lower OSI layers (e.g. ICMP, OSI layer 1 and 2 mechanisms) must be used to detect such connectivity issues.	R	R	R	R	R	R	R
2				**IPv6**							
1	5.2.1	IPv6	IP6-000010	The product shall support dual IPv4 and IPv6 stacks as described in RFC 4213.	R	R	R	R	R	R	R
2	5.2.1	IPv6	IP6-000020	Dual-stack end points or Call Connection Agents (CCAs) shall be configured to choose IPv4 over IPv6.	R	R	R	R	R	R	R
3	5.2.1	IPv6	IP6-000030	All nodes and interfaces that are "IPv6-capable" must be carefully configured and verified that the IPv6 stack is disabled until it is deliberately enabled as part of a deliberate transition strategy. This includes the stateless autoconfiguration of link-local addresses. Nodes with multiple network interfaces may need to be separately configured per interface.	R	R	R	R	R	R	R

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
4	5.2.1	IPv6	IP6-000050	The system shall provide the same (or equivalent) functionality in IPv6 as in IPv4 consistent with the requirements in the UCR for its Approved Products List (APL) category. NOTE: This requirement applies only to products that are required to perform IPv6 functionality.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
5	5.2.1	IPv6	IP6-000060	The product shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
6	5.2.1	IPv6	IP6-000070	The product shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464. NOTE: This requirement does not mandate that the remaining sections of RFC 2464 have to be implemented.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
7	5.2.1	IPv6	IP6-000080	The product shall support Path Maximum Transmission Unit (MTU) Discovery as described in RFC 1981.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
8	5.2.1	IPv6	IP6-000090	The product shall support a minimum MTU of 1280 bytes as described in RFC 2460 and updated by RFC 5095. NOTE: Guidance on MTU requirements and settings can be found in Section 6.11.4.2, Layer 2 – Data Link Layer.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
9	5.2.1	IPv6	IP6-000100	If Path MTU Discovery is used and a "Packet Too Big" message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU, then the product shall ignore the request for the smaller MTU and shall include a fragment header in the packet. NOTE: Unlike IPv4, fragmentation in IPv6 is performed only by source nodes, not by routers along a packet's delivery path.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
10	5.2.1	IPv6	IP6-000110	The product shall not use the Flow Label field as described in RFC 2460.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
11	5.2.1	IPv6	IP6-000120	The product shall be capable of setting the Flow Label field to zero when originating a packet.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
12	5.2.1	IPv6	IP6-000140	The product shall be capable of ignoring the Flow Label field when receiving packets.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
13	5.2.1	IPv6	IP6-000150	The product shall support the IPv6 Addressing Architecture as described in RFC 4291. NOTE 1: According to "DoD IPv6 Standard Profiles For IPv6-capable Products-Supplemental Guidance" version 6.0, the use of "IPv4-mapped" addresses "on-the-wire" is discouraged due to security risks raised by inherent ambiguities. NOTE 2: As noted in National Institute of Standards and Technology (NIST) Special Publication (SP) 500-267 25, "A Profile for IPv6 in the U.S. Government – Version 1.0": The use of the old Site-Local address type (RFC3879) is deprecated. The Unique Local IPv6 Unicast Addresses (ULA) (RFC 4193) mechanism has been designed to fulfill a similar requirement. While Private Addresses are widely used in IPv4 networks, generalized ULA use and support in IPv6 are not as mature nor is their architectural desirability as well understood. For these reasons, the UC products are not required to support ULA at this time. NOTE 3: An end site is defined as an end-user (subscriber) edge network domain that requires multiple subnets/64. Therefore, vendors will not be required to support anything greater than /64, such as /116 or /126 subnet.	**R**	**R**	**R**	**R**	**R**	**R**	**R**

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
14	5.2.1	IPv6	IP6-000160	The product shall support the IPv6 Scoped Address Architecture as described in RFC 4007.	R	R	R	R	R	R	R
15	5.2.1	IPv6	IP6-000170	If a scoped address (RFC 4007) is used, then the product shall use a scope index value of zero when the default zone is intended.	C	C	C	C	C	C	C
16	5.2.1	IPv6	IP6-000280	The product shall support Neighbor Discovery for IPv6 as described in RFC 4861.	R	R	R	R	R	R	R
17	5.2.1	IPv6	IP6-000300	The product shall not set the override flag bit in the Neighbor Advertisement message for solicited advertisements for any cast addresses or solicited proxy advertisements.	R	R	R	R	R	R	R
18	5.2.1	IPv6	IP6-000310	When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache does not contain the target's entry, the advertisement shall be silently discarded.	R	R	R	R	R	R	R
19	5.2.1	IPv6	IP6-000320	When a valid "Neighbor Advertisement" message is received by the product and the product neighbor cache entry is in the INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the product shall silently discard the received advertisement.	R	R	R	R	R	R	R
20	5.2.1	IPv6	IP6-000330	When address resolution fails on a neighboring address, the entry shall be deleted from the product's neighbor cache.	R	R	R	R	R	R	R
21	5.2.1	IPv6	IP6-000340	The product shall support the ability to configure the product to ignore Redirect messages.	R	R	R	R	R	R	R
22	5.2.1	IPv6	IP6-000350	The product shall only accept Redirect messages from the same router as is currently being used for that destination. NOTE: The intent of this requirement is that if a node is sending its packets destined for location A to router X, that it can only accept a Redirect message from router X for packets destined for location A to be sent to router Z.	R	R	R	R	R	R	R
23	5.2.1	IPv6	IP6-000400	The product shall prefer routers that are reachable over routers whose reachability is suspect or unknown.	R	R	R	R	R	R	R
24	5.2.1	IPv6	IP6-000420	If the product supports stateless IP address autoconfiguration including those provided for the commercial market, then the product shall support IPv6 Stateless Address Autoconfiguration (SLAAC) for interfaces supporting UC functions in accordance with RFC 4862. NOTE 1: RFC 4862 has replaced the now-obsolete RFC 2462. The scope of RFC 2462, Section 5.5, is Creation of Global and Site-Local Addresses. The scope of RFC 4862, Section 5.5, is Creation of Global Addresses. NOTE 2: "DoD IPv6 Standard Profiles for IPv6-capable Products-Supplemental Guidance" defines Host as a PC or other end-user computer or workstation running a general-purpose operating system. NOTE 3: The UC EI platform (on which the softphone is located) may be certified to the DoD IPv6 Profile and required to support autonomous configuration, either SLAAC or DHCPv6 client.	C	C	C	C	C	C	C
25	5.2.1	IPv6	IP6-000430	If the product supports IPv6 SLAAC, then the product shall have a configurable parameter that allows the function to be enabled and disabled. Specifically, the product shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless autoconfiguration.	C	C	C	C	C	C	C

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
26	5.2.1	IPv6	IP6-000440	If the product supports IPv6 SLAAC, then the product shall have the configurable parameter set not to perform stateless autoconfiguration. NOTE: The objective of this requirement is to prevent a product from using stateless auto configuration. Stateless address autoconfiguration is focused solely on softphones since they reside on PCs.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
27	5.2.1	IPv6	IP6-000450	While nodes are not required to autoconfigure their addresses using SLAAC, all IPv6 Nodes shall support link-local address configuration and Duplicate Address Detection (DAD) as specified in RFC 4862. In accordance with RFC 4862, DAD shall be implemented and shall be on by default. Exceptions to the use of DAD are noted in the following text.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
28	5.2.1	IPv6	IP6-000460	A node MUST allow for autoconfiguration-related variable to be configured by system management for each multicast-capable interface to include DupAddrDetectTransmits where a value of zero indicates that DAD is not performed on tentative addresses as specified in RFC 4862. NOTE: Network Infrastructure Security Technical Implementation Guide (STIG) states the following: The use of Duplicate Address Detection opens up the possibility of denial of service attacks. Any node can respond to Neighbor Solicitations for a tentative address, causing the other node to reject the address as a duplicate. This attack is similar to other attacks involving the spoofing of Neighbor Discovery messages. Further, RFC 4862 states the following: By default, all addresses should be tested for uniqueness prior to their assignment to an interface for safety. The test should individually be performed on all addresses obtained manually, via stateless address autoconfiguration, or via DHCPv6. To accommodate sites that believe the overhead of performing Duplicate Address Detection outweighs its benefits, the use of Duplicate Address Detection can be disabled through the administrative setting of a per-interface configuration flag. The products may include an administrative setting to disable DAD.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
29	5.2.1	IPv6	IP6-000470	The product shall support manual assignment of IPv6 addresses.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
30	5.2.1	IPv6	IP6-000520	The product shall support the Internet Control Message Protocol (ICMP) for IPv6 as described in RFC 4443.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
31	5.2.1	IPv6	IP6-000540	The product shall support the capability to enable or disable the ability of the product to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion. NOTE: In lieu of the RFC 4443 paragraph 3.1 requirement to prohibit routers from forwarding a code 3 (address unreachable) message on point-to-point link back onto the arrival link, vendors may alternatively use a prefix length of 127 on Inter-Router Links to address ping-pong issues on non-Ethernet interfaces (the ping-pong issue is not present on Ethernet interfaces).	**R**	**R**	**R**	**R**	**R**	**R**	**R**

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
32	5.2.1	IPv6	IP6-000550	The product shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address. NOTE: The number of responses may be traffic conditioned to limit the effect of a denial of service attack.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
33	5.2.1	IPv6	IP6-000560	The product shall validate ICMPv6 messages, using the information contained in the payload, before acting on them. NOTE: The actual validation checks are specific to the upper layers and are out of the scope of this UCR. Protecting the upper layer with IPSec mitigates these attacks.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
34	5.2.1	IPv6	IP6-000680	The product shall support MLD as described in RFC 2710. NOTE: This requirement was added to ensure that Neighbor Discovery multicast requirements are met. Routers are not included in this requirement since they have to meet RFC 2710 in the preceding requirement.	**R**	**R**	**R**	**R**	**R**	**R**	**R**
35	5.2.1	IPv6	IP6-000690	If the product uses IPSec, then the product shall be compatible with the Security Architecture for the IPSec described in RFC 4301. NOTE 1: RFC 4301 mandates support for several features for which support is available in Internet Key Exchange (IKE) version 2 (IKEv2) but not in IKEv1, e.g., negotiation of a Security Association (SA) representing ranges of local and remote ports or negotiation of multiple SAs with the same selectors. However, at this time the UCR does not require the use of IKEv2. Therefore, implementation at this time of RFC 4301 will include only those features which are compatible with the use of IKEv1. NOTE 2: The interfaces required to use IPSec are defined in Section 4, Information Assurance. b. If RFC 4301 is supported, then the product shall support binding of a SA with a particular context. c. If RFC 4301 is supported, then the product shall be capable of disabling the BYPASS IPSec processing choice. NOTE: The intent of this requirement is to ensure that no packets are transmitted unless they are protected by IPSec.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
36	5.2.1	IPv6	IP6-000700	If RFC 4301 is supported, then the product shall not support the mixing of IPv4 and IPv6 in a SA.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
37	5.2.1	IPv6	IP6-000710	If RFC 4301 is supported, then the product's security association database (SAD) cache shall have a method to uniquely identify a SAD entry. NOTE: The concern is that a single SAD entry will be associated with multiple security associations. RFC 4301, Section 4.4.2, Security Association Database (SAD), describes a scenario where this could occur.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
38	5.2.1	IPv6	IP6-000720	If RFC 4301 is supported, then the product shall implement IPSec to operate with both integrity and confidentiality.	**C**	**C**	**C**	**C**	**C**	**C**	**C**
39	5.2.1	IPv6	IP6-000730	If RFC 4301 is supported, then the product shall be capable of enabling and disabling the ability of the product to send an ICMP message informing the sender that an outbound packet was discarded.	**C**	**C**	**C**	**C**	**C**	**C**	**C**

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
40	5.2.1	IPv6	IP6-000740	If an ICMP outbound packet message is allowed, then the product shall be capable of rate limiting the transmission of ICMP responses.	C	C	C	C	C	C	C
41	5.2.1	IPv6	IP6-000750	If RFC 4301 is supported, then the system's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.	C	C	C	C	C	C	C
42	5.2.1	IPv6	IP6-000760	[Alarm] If RFC 4301 is supported, and the product receives a packet that does not match any SPD cache entries, and the product determines it should be discarded, then the product shall log the event and include the date/time, Security Parameter Index (SPI) if available, IPSec protocol if available, source and destination of the packet, and any other selector values of the packet. NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).	C	C	C	C	C	C	C
43	5.2.1	IPv6	IP6-000770	[Alarm] If RFC 4301 is supported, then the product should include a management control to allow an administrator to enable or disable the ability of the product to send an IKE notification of an INVALID_SELECTORS. NOTE: Some products may not be able to log all this information (e.g., the product may not have access to this information).	C	C	C	C	C	C	C
44	5.2.1	IPv6	IP6-000780	If RFC 4301 is supported, then the product shall support the ESP Protocol in accordance with RFC 4303.	C	C	C	C	C	C	C
45	5.2.1	IPv6	IP6-000790	If RFC 4303 is supported, then the product shall be capable of enabling anti-replay.	C	C	C	C	C	C	C
46	5.2.1	IPv6	IP6-000800	If RFC 4303 is supported, then the product shall check, as its first check, after a packet has been matched to its SA whether the packet contains a sequence number that does not duplicate the sequence number of any other packet received during the life of the security association.	C	C	C	C	C	C	C
47	5.2.1	IPv6	IP6-000810	If RFC 4301 is supported, then the product shall support IKEv1 as defined in RFC 2409. NOTE: The IKEv1 requirements are found in Section 4, Information Assurance.	C	C	C	C	C	C	C
48	5.2.1	IPv6	IP6-000820	To prevent a Denial of Services (DoS) attack on the initiator of an IKE_SA, the initiator shall accept multiple responses to its first message, treat each as potentially legitimate, respond to it, and then discard all the invalid half-open connections when it receives a valid cryptographically protected response to any one of its requests. Once a cryptographically valid response is received, all subsequent responses shall be ignored whether or not they are cryptographically valid.	C	C	C	C	C	C	C
49	5.2.1	IPv6	IP6-000830	If RFC 4301 is supported, then the product shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407.	C	C	C	C	C	C	C
50	5.2.1	IPv6	IP6-000840	If RFC 4301 is supported, then the product shall support the ISAKMP as defined in RFC 2408.	C	C	C	C	C	C	C
51	5.2.1	IPv6	IP6-000850	If the product supports the IPSec Authentication Header Mode, then the product shall support the IP Authentication Header (AH) as defined in RFC 4302.	C	C	C	C	C	C	C

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
52	5.2.1	IPv6	IP6-000860	If RFC 4301 is supported, then the product shall support manual keying of IPSec.	C	C	C	C	C	C	C
53	5.2.1	IPv6	IP6-000870	If RFC 4301 is supported, then the product shall support the ESP and AH cryptographic algorithm implementation requirements as defined RFC 4835	C	C	C	C	C	C	C
54	5.2.1	IPv6	IP6-000880	If RFC 4301 is supported, then the product shall support the IKEv1 security algorithms as defined in RFC 4109.	C	C	C	C	C	C	C
55	5.2.1	IPv6	IP6-000990	If the product uses Uniform Resource Identifiers (URIs) in combination with IPv6, then the product shall use the URI syntax described in RFC 3986.	C	C	C	C	C	C	C
56	5.2.1	IPv6	IP6-001010	For traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 kbps (each direction) for each IPv6 call. This is based on G.711 (20 ms codec) with IP overhead (100 kbps) resulting in a 250-byte bearer packet plus 10 kbps for signaling, Ethernet Interframe Gap, and the Secure Real-Time Transport Control Protocol (SRTCP) overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.	R	R	R	R	R	R	R
57	5.2.1	IPv6	IP6-001040	The product shall forward packets using the same IP version as the version in the received packet. NOTE: If the packet was received as an IPv6 packet, then the appliance will forward it as an IPv6 packet. If the packet was received as an IPv4 packet, then the appliance will forward the packet as an IPv4 packet. This requirement is primarily associated with the signaling packets to ensure that translation does not occur.	R	R	R	R	R	R	R
58	5.2.1	IPv6	IP6-001060	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is a unicast address, then the product shall support generation and processing of unicast IPv6 addresses having the following formats: ☐ x:x:x:x:x:x:x:x (where x is the hexadecimal values of the eight 16-bit pieces of the address). Example: 1080:0:0:0:8:800:200C:417A. ☐ x:x:x:x:x:x:d.d.d.d (where x is the hexadecimal values of the six high-order 16-bit pieces of the address, and d is the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). For example, 1080:0:0:0:8:800:116.23.135.22.	C	C	C	C	C	C	C
59	5.2.1	IPv6	IP6-001070	If the product is using AS-SIP, then the product shall support the generation and processing of IPv6 unicast addresses using compressed zeros consistent with one of the following formats: ☐ x:x:x:x:x:x:x:x format: 1080:0:0:0:8:800:200C:417A. ☐ x:x:x:x:x:x:d.d.d.d format: 1080:0:0:0:8:800:116.23.135.22. ☐ compressed zeros: 1080::8:800:200C:417A.	C	C	C	C	C	C	C

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
60	5.2.1	IPv6	IP6-001080	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is a multicast group address (i.e., the two most significant hexadecimal digits are FF), then the product shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.	C	C	C	C	C	C	C
61	5.2.1	IPv6	IP6-001090	If the product is using AS-SIP, and the <addrtype> is IPv6, then the product shall support the use of RFC 4566 for IPv6 in SDP as described in AS-SIP 2013, Section 4, SIP Requirements for AS-SIP Signaling Appliances and AS-SIP EIs.	C	C	C	C	C	C	C
62	5.2.1	IPv6	IP6-001100	If the product is using AS-SIP, and the <addrtype> is IPv6, and the <connection-address> is an IPv6 multicast group address, then the multicast connection address shall not have a Time To Live (TTL) value appended to the address as IPv6 multicast does not use TTL scoping.	C	C	C	C	C	C	C
63	5.2.1	IPv6	IP6-001110	If the product is using AS-SIP, then the product shall support the processing of IPv6 multicast group addresses having the <number of address> field and may support generating the <number of address> field. This field has the identical format and operation as the IPv4 multicast group addresses.	C	C	C	C	C	C	C
64	5.2.1	IPv6	IP6-001120	The product shall be able to provide topology hiding [e.g., Network Address Translation (NAT)] for IPv6 packets as described in Section 4, Information Assurance. NOTE: Deployments requiring the network topology hiding that IPv4 NAT provided as a side-effect should consider RFC 4864 – Local Network Protection (LNP) for IPv6.	R	R	R	R	R	R	R
65	5.2.1	IPv6	IP6-001140	If the product supports Remote Authentication Dial-in User Service (RADIUS) authentication, then the product shall support RADIUS as defined in RFC 3162.	C	C	C	C	C	C	C
66	5.2.1	IPv6	IP6-001150	The products shall support Differentiated Services as described in RFC 2474 for a voice and video stream in accordance with Section 2, Session Control Products, and Section 6, Network Infrastructure End-to-End Performance, plain text DSCP plan.	R	R	R	R	R	R	R
67	5.2.2	IPv6	Table 5.2-7	Security device product shall meet the RFCs in Table 5.2-7	R	R	R	R	R	R	R
3	**Security Device Requirements**										
3.1	**Conformance**										
1	13.2.1	Conformance	SEC-000010	The security device shall conform to all of the MUST requirements found in Request for Change (RFC) 3948, "UDP Encapsulation of IPSec Packets."	R	N/A	N/A	N/A	N/A	N/A	N/A
3.2	**General**										
1	13.2.2	General	SEC-000020	The security device must support NTPv3 for interoperability.	R	R	R	N/A	R	R	N/A
2	13.2.2	General	SEC-000030	The security device shall be managed from a central place, clients, and servers.	R	N/A	N/A	N/A	N/A	R	N/A
3	13.2.2	General	SEC-000040	The security device shall properly implement an ordered list policy procedure.	R	R	R	N/A	N/A	N/A	N/A
4	13.2.2	General	SEC-000050	The security device shall apply a set of rules in monitoring events and based on these rules indicate a potential violation of the security device security policy.	N/A	R	R	N/A	N/A	R	N/A

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
5	13.2.2	General	SEC-000060	An automated, continuous online monitoring and audit trail creation capability is deployed with the capability to immediately alert personnel of any unusual or inappropriate activity with potential Information Assurance implications.	R	R	R	N/A	N/A	N/A	N/A
6	13.2.2	General	SEC-000070	If the security device allows configuration of access settings, the security device shall provide minimum recorded security-relevant events including any activity caught by the "deny all" rule at the end of the security device rule base.	N/A	R	R	N/A	R	N/A	N/A
7	13.2.2	General	SEC-000080	The security device shall log matches to filter rules that deny access when configured to do so.	N/A	R	N/A	N/A	N/A	N/A	N/A
8	13.2.2	General	SEC-000090	The security device shall log an information flow between a source subject and a destination subject via a controlled operation if the information security attributes match the attributes in an information flow policy rule (contained in the information flow policy)	R	N/A	R	N/A	N/A	N/A	N/A
9	13.2.2	General	SEC-000100	The security device shall log data and audit events when a replay is detected.	R	N/A	R	N/A	N/A	N/A	N/A
10	13.2.2	General	SEC-000110	The security device shall be able to collect the following: Identification, Authentication, and Authorization events.	R	N/A	R	N/A	R	N/A	N/A
11	13.2.2	General	SEC-000120	The security device shall be able to collect network traffic.	R	N/A	R	N/A	R	N/A	N/A
12	13.2.2	General	SEC-000130	The security device shall be able to collect detected known vulnerabilities.	R	N/A	R	N/A	R	N/A	N/A
13	13.2.2	General	SEC-000140	The security device's controlled interface shall be configured such that its operational failure or degradation shall not result in any unauthorized release of information outside the Information Security (IS) perimeter nor result in any external information entering the IS perimeter.	R	R	R	N/A	N/A	R	N/A
14	13.2.2	General	SEC-000150	The security device must protect itself against attempts by unauthorized users to bypass, deactivate, or tamper with security device security functions.	R	R	R	N/A	R	R	N/A
15	13.2.2	General	SEC-000160	The security device shall drop all packets with an IPv4 source address of all zeros.	R	R	R	N/A	N/A	R	N/A
16	13.2.2	General	SEC-000170	The security device shall drop all traffic from the internal network that does not use a legitimate internal address range as its source address.	R	R	R	N/A	N/A	R	N/A
17	13.2.2	General	SEC-000180	The security device shall pass traffic, which the security device has not identified as being a security problem, without altering the contents, except as necessary to perform functions such as Network Address Translation (NAT).	N/A	R	R	N/A	R	N/A	N/A
18	13.2.2	General	SEC-000190	A security device shall prevent all known network-based current attack techniques (Common Vulnerabilities and Exploits) from compromising the security device.	N/A	R	R	N/A	R	N/A	N/A
19	13.2.2	General	SEC-000200	The security device shall mediate the flow of all information between a user on an internal network connected to the security device and a user on an external network connected to the security device and must ensure that residual information from a previous information flow is not transmitted.	N/A	R	R	N/A	N/A	N/A	N/A
20	13.2.2	General	SEC-000210	The security device shall reject requests for access or services in which the presumed source identity of the source subject is an external Information Technology (IT) entity on a broadcast network.	R	R	R	N/A	N/A	R	N/A
21	13.2.2	General	SEC-000220	The security device shall detect replay attacks using either security device data or security attributes.	R	N/A	R	N/A	R	R	N/A

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
22	13.2.2	General	SEC-000230	The security device shall ensure that the security policy enforcement functions are invoked and succeed before each function within the security functions scope of control is allowed to proceed.	R	R	R	N/A	N/A	N/A	N/A
23	13.2.2	General	SEC-000240	The security device shall enforce System Administrator policy regarding Instant Messaging traffic.	N/A	R	N/A	N/A	N/A	N/A	N/A
24	13.2.2	General	SEC-000250	The security device shall enforce System Administrator policy regarding Voice and Video over Internet Protocol (VVoIP) traffic.	N/A	R	N/A	N/A	N/A	N/A	N/A
25	13.2.2	General	SEC-000260	The controlled interface shall provide the ability to restore its functionality fully in accordance with documented restoration procedures.	R	R	R	N/A	N/A	R	N/A
26	13.2.2	General	SEC-000270	Each controlled interface shall be configured to ensure that all (incoming and outgoing) communications protocols, services, and communications not explicitly permitted are prohibited.	N/A	N/A	R	N/A	N/A	N/A	N/A
27	13.2.2	General	SEC-000280	The security device shall provide a high availability failover capability that maintains state. This capability shall be configurable.	R	R	R	N/A	N/A	R	N/A
28	13.2.2	General	SEC-000290	Fails.	R	R	R	N/A	N/A	R	N/A
29	13.2.2	General	SEC-000300	Is attacked.	R	R	R	N/A	N/A	R	N/A
30	13.2.2	General	SEC-000310	Storage becomes exhausted.	R	R	N/A	N/A	N/A	R	N/A
31	13.2.2	General	SEC-000320	Fails to restart/reboot.	R	R	N/A	N/A	N/A	R	N/A
3.3				**Performance**							
1	13.2.3	Performance	SEC-000330	The developer must specify the security device's bandwidth requirements and capabilities. This shall include the maximum bandwidth speeds the device will operate on as well as the security device bandwidth requirements (bandwidth in kbps) documented by whom the device communicates with, frequency, and kbps transmitted and received (e.g., product downloads, signature files).	R	R	R	N/A	R	N/A	N/A
2	13.2.3	Performance	SEC-000340	The security device, as configured, must process new connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.	R	R	R	N/A	N/A	N/A	N/A
3	13.2.3	Performance	SEC-000350	The security device, as configured, must process new hypertext transport protocol (HTTP) connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.	R	R	R	N/A	N/A	N/A	N/A
4	13.2.3	Performance	SEC-000360	The security device, as configured, must process new secure file transfer protocol (FTP) connections at the rate of the expected maximum number of connections as advertised by the vendor within a 1-minute period.	R	R	R	N/A	N/A	N/A	N/A
5	13.2.3	Performance	SEC-000370	The security device shall use a commercial best practice defensive solution and maintain advertised normal operation packet loss rates for all legitimate data packets when under a SYN Flood attack.	R	R	R	N/A	R	N/A	N/A
6	13.2.3	Performance	SEC-000380	The security device shall demonstrate a latency variance of less than 20 percent and a packet loss variance of less than 10 percent of the manufacturer-specified nominal values for all operational conditions.	N/A	R	N/A	N/A	N/A	N/A	N/A
3.4				**Functionality**							
1	13.2.4	Functionality	SEC-000390	The security device shall enforce the policy pertaining to any indication of a potential security violation.	R	R	N/A	N/A	N/A	N/A	N/A
2	13.2.4	Functionality	SEC-000400	The security device shall be configurable to perform actions based on different information flow policies.	R	R	N/A	N/A	N/A	N/A	N/A

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
3	13.2.4	Functionality	SEC-000410	The security device shall deny establishment of an authorized user session based on network source (i.e., source IP address).	R	R	N/A	N/A	N/A	N/A	N/A
4	13.2.4	Functionality	SEC-000420	The security device shall enforce the System Administrator's specified maximum quota of transport-layer open connections that a source subject identifier can use over a specified period.	N/A	R	N/A	N/A	N/A	N/A	N/A
5	13.2.4	Functionality	SEC-000430	The security device shall enforce the System Administrator's policy options pertaining to network traffic violations to a specific TCP port within a specified period.	R	R	N/A	N/A	N/A	N/A	N/A
6	13.2.4	Functionality	SEC-000440	The security device shall enforce the System Administrator's policy options pertaining to violations of network traffic rules within a specified period.	R	R	N/A	N/A	N/A	N/A	N/A
7	13.2.4	Functionality	SEC-000450	The security device shall enforce the System Administrator's policy options pertaining to any security device-detected replay of data and/or nested security attributes.	R	R	N/A	N/A	N/A	N/A	N/A
8	13.2.4	Functionality	SEC-000460	The security device shall provide the ability to push policy to the VPN client and the ability to monitor the client's activity.	R	N/A	N/A	N/A	N/A	N/A	N/A
9	13.2.4	Functionality	SEC-000470	The security device shall have five Ethernet ports, one pair for primary ingress and egress, one pair for backup, and one for out-of-band management (OOBM).	N/A	R	N/A	N/A	N/A	N/A	N/A
10	13.2.4	Functionality	SEC-000480	The security device, when configured, shall log the event of dropping packets and the reason for dropping them.	N/A	R	N/A	N/A	N/A	N/A	N/A
11	13.2.4	Functionality	SEC-000490	At a minimum, the following confidentiality policy adjudication features shall be provided for each controlled interface. Encrypt, as needed, all outgoing communication including the body and attachment of the communication.	R	N/A	N/A	N/A	N/A	N/A	N/A
12	13.2.4	Functionality	SEC-000500	A security device shall properly enforce the TCP state.	N/A	R	N/A	N/A	N/A	N/A	N/A
13	13.2.4	Functionality	SEC-000510	A security device shall properly accept and deny traffic based on multiple rules.	N/A	R	N/A	N/A	N/A	N/A	N/A
14	13.2.4	Functionality	SEC-000520	A security device will apply filtering to the service UDP echo (port 7).	N/A	R	N/A	N/A	N/A	N/A	N/A
15	13.2.4	Functionality	SEC-000530	A security device will apply filtering to the service UDP discard (port 9).	N/A	R	N/A	N/A	N/A	N/A	N/A
16	13.2.4	Functionality	SEC-000540	A security device will apply filtering to the service UDP chargen (port 19).	N/A	R	N/A	N/A	N/A	N/A	N/A
17	13.2.4	Functionality	SEC-000550	A security device will apply filtering to the service UDP TCPMUX (port 1).	N/A	R	N/A	N/A	N/A	N/A	N/A
18	13.2.4	Functionality	SEC-000560	A security device will apply filtering to the service UDP daytime (port 13).	N/A	R	N/A	N/A	N/A	N/A	N/A
19	13.2.4	Functionality	SEC-000570	A security device will apply filtering to the service UDP time (port 37).	N/A	R	N/A	N/A	N/A	N/A	N/A
20	13.2.4	Functionality	SEC-000580	A security device will apply filtering to the service UDP supdup (port 95).	N/A	R	N/A	N/A	N/A	N/A	N/A
21	13.2.4	Functionality	SEC-000590	A security device will apply filtering to the service UDP sunrpc (port 111).	N/A	R	N/A	N/A	N/A	N/A	N/A
22	13.2.4	Functionality	SEC-000600	A security device will apply filtering to the service UDP loc-srv (port 135).	N/A	R	N/A	N/A	N/A	N/A	N/A
23	13.2.4	Functionality	SEC-000610	A security device will apply filtering to the service UDP netbios-ns (port 137).	N/A	R	N/A	N/A	N/A	N/A	N/A
24	13.2.4	Functionality	SEC-000620	A security device will apply filtering to the service UDP netbios-dgm (port 138).	N/A	R	N/A	N/A	N/A	N/A	N/A
25	13.2.4	Functionality	SEC-000630	A security device will apply filtering to the service UDP netbios-ssn (port 139).	N/A	R	N/A	N/A	N/A	N/A	N/A
26	13.2.4	Functionality	SEC-000640	A security device will apply filtering to the service UDP BootP (port 67).	N/A	R	N/A	N/A	N/A	N/A	N/A
27	13.2.4	Functionality	SEC-000650	A security device will apply filtering to the service UDP TFTP (port 69).	N/A	R	N/A	N/A	N/A	N/A	N/A
28	13.2.4	Functionality	SEC-000660	A security device will apply filtering to the service UDP XDMCP (port 177).	N/A	R	N/A	N/A	N/A	N/A	N/A

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
29	13.2.4	Functionality	SEC-000670	A security device will apply filtering to the service UDP syslog (port 514).	N/A	R	N/A	N/A	N/A	N/A	N/A
30	13.2.4	Functionality	SEC-000680	A security device will apply filtering to the service UDP talk (port 517).	N/A	R	N/A	N/A	N/A	N/A	N/A
31	13.2.4	Functionality	SEC-000690	A security device will apply filtering to the service UDP ntalk (port 518).	N/A	R	N/A	N/A	N/A	N/A	N/A
32	13.2.4	Functionality	SEC-000700	A security device will apply filtering to the service UDP MS SQL Server (port 1434).	N/A	R	N/A	N/A	N/A	N/A	N/A
33	13.2.4	Functionality	SEC-000710	A security device will apply filtering to the service UDP MS UPnP SSDP (port 5000).	N/A	R	N/A	N/A	N/A	N/A	N/A
34	13.2.4	Functionality	SEC-000720	A security device will apply filtering to the service UDP NFS (port 2049).	N/A	R	N/A	N/A	N/A	N/A	N/A
35	13.2.4	Functionality	SEC-000730	A security device will apply filtering to the service UDP Back Orifice (port 31337).	N/A	R	N/A	N/A	N/A	N/A	N/A
36	13.2.4	Functionality	SEC-000740	A security device will apply filtering to the service TCP TCPMUX (port 1).	N/A	R	N/A	N/A	N/A	N/A	N/A
37	13.2.4	Functionality	SEC-000750	A security device will apply filtering to the service TCP echo (port 7).	N/A	R	N/A	N/A	N/A	N/A	N/A
38	13.2.4	Functionality	SEC-000760	A security device will apply filtering to the service TCP discard (port 9).	N/A	R	N/A	N/A	N/A	N/A	N/A
39	13.2.4	Functionality	SEC-000770	A security device will apply filtering to the service TCP systat (port 11).	N/A	R	N/A	N/A	N/A	N/A	N/A
40	13.2.4	Functionality	SEC-000780	A security device will apply filtering to the service TCP daytime (port 13).	N/A	R	N/A	N/A	N/A	N/A	N/A
41	13.2.4	Functionality	SEC-000790	A security device will apply filtering to the service TCP netstat (port 15).	N/A	R	N/A	N/A	N/A	N/A	N/A
42	13.2.4	Functionality	SEC-000800	A security device will apply filtering to the service TCP chargen (port 19).	N/A	R	N/A	N/A	N/A	N/A	N/A
43	13.2.4	Functionality	SEC-000810	A security device will apply filtering to the service TCP time (port 37).	N/A	R	N/A	N/A	N/A	N/A	N/A
44	13.2.4	Functionality	SEC-000820	A security device will apply filtering to the service TCP whois (port 43).	N/A	R	N/A	N/A	N/A	N/A	N/A
45	13.2.4	Functionality	SEC-000830	A security device will apply filtering to the service TCP supdup (port 95).	N/A	R	N/A	N/A	N/A	N/A	N/A
46	13.2.4	Functionality	SEC-000840	A security device will apply filtering to the service TCP sunrpc (port 111).	N/A	R	N/A	N/A	N/A	N/A	N/A
47	13.2.4	Functionality	SEC-000850	A security device will apply filtering to the service TCP loc-srv (port 135).	N/A	R	N/A	N/A	N/A	N/A	N/A
48	13.2.4	Functionality	SEC-000860	A security device will apply filtering to the service TCP netbios-ns (port 137).	N/A	R	N/A	N/A	N/A	N/A	N/A
49	13.2.4	Functionality	SEC-000870	A security device will apply filtering to the service TCP netbios-dgm (port 138).	N/A	R	N/A	N/A	N/A	N/A	N/A
50	13.2.4	Functionality	SEC-000880	A security device will apply filtering to the service TCP netbios-ssn (port 139).	N/A	R	N/A	N/A	N/A	N/A	N/A
51	13.2.4	Functionality	SEC-000890	A security device will apply filtering to the service TCP netbios-ds (port 445).	N/A	R	N/A	N/A	N/A	N/A	N/A
52	13.2.4	Functionality	SEC-000900	A security device will apply filtering to the service TCP rexec (port 512).	N/A	R	N/A	N/A	N/A	N/A	N/A
53	13.2.4	Functionality	SEC-000910	A security device will apply filtering to the service TCP lpr (port 515).	N/A	R	N/A	N/A	N/A	N/A	N/A
54	13.2.4	Functionality	SEC-000920	A security device will apply filtering to the service TCP uucp (port 540).	N/A	R	N/A	N/A	N/A	N/A	N/A
55	13.2.4	Functionality	SEC-000930	A security device will apply filtering to the service TCP Microsoft UPnP System Services Delivery Point (SSDP) (port 1900).	N/A	R	N/A	N/A	N/A	N/A	N/A
56	13.2.4	Functionality	SEC-000940	A security device will apply filtering to the service TCP X-Window System (ports 6000–6063).	N/A	R	N/A	N/A	N/A	N/A	N/A
57	13.2.4	Functionality	SEC-000950	A security device will apply filtering to the service TCP IRC (port 6667).	N/A	R	N/A	N/A	N/A	N/A	N/A
58	13.2.4	Functionality	SEC-000960	A security device will apply filtering to the service TCP NetBus (ports 12345–12346).	N/A	R	N/A	N/A	N/A	N/A	N/A
59	13.2.4	Functionality	SEC-000970	A security device will apply filtering to the service TCP Back Orifice (port 31337).	N/A	R	N/A	N/A	N/A	N/A	N/A
60	13.2.4	Functionality	SEC-000980	A security device will apply filtering to the service TCP finger (port 79).	N/A	R	N/A	N/A	N/A	N/A	N/A
61	13.2.4	Functionality	SEC-000990	A security device will apply filtering to the service TCP SNMP (port 161).	N/A	R	N/A	N/A	N/A	N/A	N/A
62	13.2.4	Functionality	SEC-001000	A security device will apply filtering to the service UDP SNMP (port 161).	N/A	R	N/A	N/A	N/A	N/A	N/A

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
63	13.2.4	Functionality	SEC-001010	A security device will apply filtering to the service TCP SNMP trap (port 162).	N/A	R	N/A	N/A	N/A	N/A	N/A
64	13.2.4	Functionality	SEC-001020	A security device will apply filtering to the service UDP SNMP trap (port 162).	N/A	R	N/A	N/A	N/A	N/A	N/A
65	13.2.4	Functionality	SEC-001030	A security device will apply filtering to the service TCP rlogin (port 513).	N/A	R	N/A	N/A	N/A	N/A	N/A
66	13.2.4	Functionality	SEC-001040	A security device will apply filtering to the service UDP who (port 513).	N/A	R	N/A	N/A	N/A	N/A	N/A
67	13.2.4	Functionality	SEC-001050	A security device will apply filtering to the service TCP rsh, rcp, rdist, and rdump (port 514).	N/A	R	N/A	N/A	N/A	N/A	N/A
68	13.2.4	Functionality	SEC-001060	A security device will apply filtering to the service TCP new who (port 550).	N/A	R	N/A	N/A	N/A	N/A	N/A
69	13.2.4	Functionality	SEC-001070	A security device will apply filtering to the service UDP new who (port 550).	N/A	R	N/A	N/A	N/A	N/A	N/A
70	13.2.4	Functionality	SEC-001080	A security device will apply filtering to the service Network Time Protocol (NTP).	N/A	R	N/A	N/A	N/A	N/A	N/A
71	13.2.4	Functionality	SEC-001090	A security device will apply filtering to the service Cisco Discovery Protocol (CDP).	N/A	R	N/A	N/A	N/A	N/A	N/A
72	13.2.4	Functionality	SEC-001100	A security device will apply filtering to Voice and Video Services (UC SIP), H.323, and RSVP.	N/A	R	N/A	N/A	N/A	N/A	N/A
73	13.2.4	Functionality	SEC-001110	A security device will apply filtering to the service UDP SRTP (SRTCP) and RTCP.	N/A	R	N/A	N/A	N/A	N/A	N/A
74	13.2.4	Functionality	SEC-001120	A security device will apply filtering to the service DSCP.	N/A	R	N/A	N/A	N/A	N/A	N/A
75	13.2.4	Functionality	SEC-001130	The security device shall detect and protect against a focused method of attack: Footprinting and Scanning.	N/A	N/A	R	N/A	N/A	N/A	N/A
76	13.2.4	Functionality	SEC-001140	The security device shall detect and protect against a focused method of attack: Enumeration.	N/A	N/A	R	N/A	N/A	N/A	N/A
77	13.2.4	Functionality	SEC-001150	The security device shall detect and protect against a focused method of attack: Gaining Access.	N/A	N/A	R	N/A	N/A	N/A	N/A
78	13.2.4	Functionality	SEC-001160	The security device shall detect and protect against a focused method of attack: Escalation of Privilege.	N/A	N/A	R	N/A	N/A	N/A	N/A
79	13.2.4	Functionality	SEC-001170	The security device shall detect and protect against a focused method of attack: Network Exploitation.	N/A	N/A	R	N/A	N/A	N/A	N/A
80	13.2.4	Functionality	SEC-001180	The security device shall detect and protect against a focused method of attack: Cover Tracks.	N/A	N/A	R	N/A	N/A	N/A	N/A
81	13.2.4	Functionality	SEC-001190	The security device shall have the capability to provide proper notification upon detection of a potential security violation or to forward event status data to a Network Management System (NMS) that will take the appropriate action to include providing notification of the event.	N/A	N/A	R	N/A	N/A	N/A	N/A
82	13.2.4	Functionality	SEC-001200	The security device shall have the capability to alert the administrator immediately by displaying a message at the local and remote administrative consoles when an administrative session exists for each of the defined administrative roles.	N/A	N/A	R	N/A	N/A	N/A	N/A
83	13.2.4	Functionality	SEC-001210	The security device shall generate an audit record of all failures to reassemble fragmented packets.	N/A	N/A	R	N/A	R	N/A	N/A

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
84	13.2.4	Functionality	SEC-001220	The security device shall log requests in which the information received by the security device contains the route (set of host network identifiers) by which information shall flow from the source subject to the destination subject.	N/A	N/A	R	N/A	N/A	N/A	N/A
85	13.2.4	Functionality	SEC-001230	The security device shall log an information flow between a source subject and a destination subject via a controlled operation if the source subject has successfully authenticated to the security device.	N/A	N/A	R	N/A	N/A	N/A	N/A
86	13.2.4	Functionality	SEC-001240	The security device shall reject data when a replay is detected.	N/A	N/A	R	N/A	N/A	N/A	N/A
87	13.2.4	Functionality	SEC-001250	The device shall support the capability to detect and send alarms in responses to threats identified in VVoIP signaling.	N/A	N/A	O	N/A	N/A	N/A	N/A
88	13.2.4	Functionality	SEC-001260	The IPS shall support the capability to detect an abnormal number of 401/407 UC SIP response messages, indicating that a possibly unauthorized user or device is attempting to connect to the system.	N/A	N/A	O	N/A	N/A	N/A	N/A
89	13.2.4	Functionality	SEC-001270	The IPS shall support the capability to detect when an abnormal time-out for a UC SIP request occurs (e.g., large numbers of repeated UC SIP requests or responses, unusual number of UC SIP requests sent with no matching response). NOTE: If a UC SIP request time-out occurs, it could be an indication that the system has failed because of a denial of service (DoS) attack resulting from a maliciously crafted request.	N/A	N/A	O	N/A	N/A	N/A	N/A
90	13.2.4	Functionality	SEC-001280	The device shall support the capability to detect when UC SIP messages exceed a configurable maximum message length.	N/A	N/A	O	N/A	N/A	N/A	N/A
91	13.2.4	Functionality	SEC-001290	The device shall support the capability to detect when a UC SIP message contains nonprintable characters. NOTE: The presence of nonprintable characters could indicate an attempt by an adversary to insert executable code or cause abnormal behavior in a system.	N/A	N/A	O	N/A	N/A	N/A	N/A
92	13.2.4	Functionality	SEC-001300	The device shall support the capability to detect attempts to inject SQL queries into UC SIP signaling messages.	N/A	N/A	O	N/A	N/A	N/A	N/A
93	13.2.4	Functionality	SEC-001310	The device shall support the capability to detect unusual IPv4 or IPv6 addresses contained in UC SIP messages (e.g., the local host/loopback address, link local addresses).	N/A	N/A	O	N/A	N/A	N/A	N/A
94	13.2.4	Functionality	SEC-001320	The device shall support the capability to detect traffic that does not have the characteristics of UC SIP traffic, but is still sent over a channel established for sending UC SIP messages (e.g., strings of characters that are not UC SIP related).	N/A	N/A	O	N/A	N/A	N/A	N/A
95	13.2.4	Functionality	SEC-001330	The device shall support the capability to detect and send alarms in response to threats identified in VVoIP media traffic and other traffic that flows across the Session Border Controller (SBC) boundary.	N/A	N/A	O	N/A	N/A	N/A	N/A
96	13.2.4	Functionality	SEC-001340	The device shall detect attempts to inject packets into a media stream or perform replay attacks [e.g., duplicate sequence numbers appearing in an real-time transport protocol (RTP) stream].	N/A	N/A	O	N/A	N/A	N/A	N/A
97	13.2.4	Functionality	SEC-001350	The device shall support the capability to detect traffic that should be VVoIP traffic based on its headers, but does not have the characteristics of a VVoIP traffic stream.	N/A	N/A	O	N/A	N/A	N/A	N/A

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
98	13.2.4	Functionality	SEC-001360	The device shall support the capability to detect signatures associated with the presence of data, files, executables, SQL commands, viruses, or other unusual data contained within a media stream intended for VVoIP.	N/A	N/A	O	N/A	N/A	N/A	N/A
99	13.2.4	Functionality	SEC-001370	The device shall support the capability to detect abnormally sized packets in the VVoIP media stream.	N/A	N/A	O	N/A	N/A	N/A	N/A
100	13.2.4	Functionality	SEC-001380	At a minimum, the device shall support the capability to detect unusually large packets associated with the codec types specified in Section 2.9, End Instruments. NOTE: This requires the device to support the capability to recognize the codec that should b	N/A	N/A	O	N/A	N/A	N/A	N/A
101	13.2.4	Functionality	SEC-001390	The device shall support the capability to receive periodic VVoIP signaling, media, and other threat signature updates from an authenticated source in an automated manner.	N/A	N/A	O	N/A	N/A	N/A	N/A
102	13.2.4	Functionality	SEC-001400	The device shall ensure that each function implemented shall be logically separate from the other functions.	N/A	N/A	N/A	R	N/A	N/A	N/A
103	13.2.4	Functionality	SEC-001410	The device must comply with all applicable UCR requirements for any implemented functions.	N/A	N/A	N/A	R	N/A	N/A	N/A
104	13.2.4	Functionality	SEC-001420	The system shall be able to authenticate all devices before allowing access to the network.	N/A	N/A	N/A	N/A	N/A	R	N/A
105	13.2.4	Functionality	SEC-001430	The system shall be capable of denying access to any device that fails authentication.	N/A	N/A	N/A	N/A	N/A	R	N/A
106	13.2.4	Functionality	SEC-001440	The system shall support 802.1X-based policy enforcement points and Layer 3 policy enforcement points with 802.1X-based policy enforcement preferred.	N/A	N/A	N/A	N/A	N/A	R	N/A
107	13.2.4	Functionality	SEC-001450	The system shall operate in both in-band and out-of-band modes to support network segments that both can and cannot utilize 802.1X.	N/A	N/A	N/A	N/A	N/A	R	N/A
108	13.2.4	Functionality	SEC-001460	The system shall allow an administrator to override the authentication assessment and allow or deny a device to enter the authorized network.	N/A	N/A	N/A	N/A	N/A	R	N/A
109	13.2.4	Functionality	SEC-001470	The system shall provide the administrator with a means for configuring exception policies to accommodate authorized devices that do not support NAC agents or other means for authentication such as 802.1X.	N/A	N/A	N/A	N/A	N/A	R	N/A
110	13.2.4	Functionality	SEC-001480	The system shall allow security managers and administrators the ability to create, manipulate, and maintain multiple device NAC policies for different classes of devices.	N/A	N/A	N/A	N/A	N/A	R	N/A
111	13.2.4	Functionality	SEC-001490	The system shall be capable of being configured for both distributed NAC policy and localized NAC policy enforcement administration.	N/A	N/A	N/A	N/A	N/A	R	N/A
112	13.2.4	Functionality	SEC-001500	The system shall allow an administrator to manually configure event publication; e.g., set filters on event types to be displayed, alerted.	N/A	N/A	N/A	N/A	N/A	R	N/A
113	13.2.4	Functionality	SEC-001510	The system shall have the ability to be configured to log, but not enforce, NAC policies. The system shall provide the ability to log and notify, but not enforce, optionally all of the following: compliance OR device authentication OR remediation notifications.	N/A	N/A	N/A	N/A	N/A	R	N/A
114	13.2.4	Functionality	SEC-001520	The system shall provide the capability to either turn off or disable the NAC functionality globally, and on a NAC-controlled interface basis.	N/A	N/A	N/A	N/A	N/A	R	N/A
115	13.2.4	Functionality	SEC-001530	The system shall allow administrators to receive information on a device's NAC status.	N/A	N/A	N/A	N/A	N/A	R	N/A

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
116	13.2.4	Functionality	SEC-001540	The system shall be capable of placing the end user machine into an alternate network (quarantine) if the end user machine is not authorized to connect to the trusted network, regardless of its enforcement method. NOTE: The network components [e.g., VPN, Local Area Network (LAN) Server] must be configured so that end devices do not have access to other untrusted devices while quarantined.	N/A	N/A	N/A	N/A	N/A	R	N/A
117	13.2.4	Functionality	SEC-001550	The system shall allow isolated segments of the network to be designated for clients that meet a specified configuration policy compliance status.	N/A	N/A	N/A	N/A	N/A	R	N/A
118	13.2.4	Functionality	SEC-001560	For all devices, the system shall support the capability to remove an asset from the group of its managed assets without sympathetic errors (e.g., popup window saying "invalid command"), thus allowing the user to remove managed devices without issue.	N/A	N/A	N/A	N/A	N/A	R	N/A
119	13.2.4	Functionality	SEC-001570	The system shall require an authentication procedure to process new clients requesting downloads.	N/A	N/A	N/A	N/A	N/A	R	N/A
120	13.2.4	Functionality	SEC-001580	The system shall support the capability to allow end devices to automatically and securely download required patches or software when the device is found to be non-compliant. Any NAC agent functionality shall support the capability to install downloaded patches manually.	N/A	N/A	N/A	N/A	N/A	R	N/A
121	13.2.4	Functionality	SEC-001590	The system's remediation checks shall be customizable by security managers and administrators.	N/A	N/A	N/A	N/A	N/A	R	N/A
122	13.2.4	Functionality	SEC-001600	The system shall not interfere with the operation of DOD-approved antivirus software (e.g., Symantec and McAfee), Host-Based Security System (HBSS), and Federal Desktop Core Configuration (FDCC). NOTE: Interoperability with HBSS is preferred.	N/A	N/A	N/A	N/A	N/A	R	N/A
123	13.2.4	Functionality	SEC-001610	The system shall be configurable to fail closed.	N/A	N/A	N/A	N/A	N/A	R	N/A
124	13.2.4	Functionality	SEC-001620	The system shall provide encrypted communications from the NAC client agent to the NAC device using Federal Information Processing Standards (FIPS)-validated encryption.	N/A	N/A	N/A	N/A	N/A	R	N/A
125	13.2.4	Functionality	SEC-001630	The system shall protect against subversive network access activity. This may be provided by interfacing with post authentication policy enforcement of third-party devices using widely- accepted technologies such as Trusted Network Control Interface – Metadata Access Point (IF-MAP) Protocol.	N/A	N/A	N/A	N/A	N/A	R	N/A
126	13.2.4	Functionality	SEC-001640	NAC management devices shall have the capability for manual and, optionally, automatic recovery from failed operations to return to normal settings/ operations/systems, to include log merging.	N/A	N/A	N/A	N/A	N/A	R	N/A
127	13.2.4	Functionality	SEC-001650	The system shall support the capability to export logs in an open standard format (e.g., Syslog).	N/A	N/A	N/A	N/A	N/A	R	N/A
128	13.2.4	Functionality	SEC-001660	The system shall provide the capability to queue events when communication is lost.	N/A	N/A	N/A	N/A	N/A	R	N/A
129	13.2.4	Functionality	SEC-001670	The system shall be capable of reporting alerts to multiple management consoles for all administratively specified events.	N/A	N/A	N/A	N/A	N/A	R	N/A
130	13.2.4	Functionality	SEC-001680	The system shall provide detailed logs of all administratively specified events.	N/A	N/A	N/A	N/A	N/A	R	N/A
131	13.2.4	Functionality	SEC-001690	The system shall have the ability to time-stamp all events using Greenwich Mean Time (GMT), to include log data, in a consistent frame of reference.	N/A	N/A	N/A	N/A	N/A	R	N/A
132	13.2.4	Functionality	SEC-001700	The product shall support a concept of operations which allows individual managers to support large numbers of distributed managed elements.	N/A	N/A	N/A	N/A	N/A	R	N/A

Table 3-5. Security Device Capability/Functional Requirements (continued)

CR/FR ID	UCR 2013 Section	Capability/Function	Requirements		VPN	FW	IPS	ISS	WIDS	NAC	IAT
133	13.2.4	Functionality	SEC-001710	The system shall allow configurable reporting, based on administrator-selected attributes/thresholds, to control how and when reports are generated.	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**R**	**N/A**
134	13.2.4	Functionality	SEC-001720	The system shall support the capability to identify connecting clients that do not have an 802.1X supplicant or NAC agent/remediation software installed.	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**R**	**N/A**
135	13.2.4	Functionality	SEC-001730	The system shall support the capability to check for syntax errors and duplicate policies before NAC policies are implemented.	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**R**	**N/A**
136	13.2.4	Functionality	SEC-001740	The system shall support the capability to integrate with and use Active Directory when authenticating connected devices.	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**R**	**N/A**
137	13.2.4	Functionality	SEC-001750	The system shall support the capability to periodically perform reauthentication and remediation in automated manner at a configurable interval.	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**R**	**N/A**
138	13.2.4	Functionality	SEC-001760	NAC systems using 802.1X must be compliant with the relevant and current Institute of Electrical and Electronics Engineers (IEEE) standards for 802.1X.	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**R**	**N/A**
139	13.2.4	Functionality	SEC-001770	The system shall have the ability to work with any Remote Authentication Dial-In User Server (RADIUS) in 802.1X enforcement mode.	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**R**	**N/A**
140	13.2.4	Functionality	SEC-001780	The system shall have the ability to support short-term client disconnections, such as taking a laptop to a meeting, and then reconnecting to the network without requiring the client to pass through the testing process.	**N/A**	**N/A**	**N/A**	**N/A**	**N/A**	**R**	**N/A**

Table 3-5. Security Device Capability/Functional Requirements (continued)

LEGEND:

AAA	Authentication, Authorization, and Accounting	IPv6	Internet Protocol version 6	RSVP	Resource Reservation Protocol
AAdmin	Audit Administrator	IS	Intermediate System	RTP	Real-Time Transport Protocol
AEI	Audio End Instrument	ISAKMP	Internet Security Association and Key Management Protocol	SA	Security Association
AES-CTR	Advanced Encryption Standard Counter Mode			SAD	Security Association Database
AH	Authentication Header	ISS	Integrated Security Solution	SBC	Session Border Controller
AIA	Authority Information Access	IT	Information Technology	SC	Session Controller
APL	Approved Products List	KEXINIT	Key Exchange Initialization	SDP	Session Description Protocol
AS-SIP	Assured Services Session Initiation Protocol	LAN	Local Area Network	SEC	Security
C	Conditional	LDAP	Lightweight Directory Access Protocol	SHA	Secure Hash Algorithm
CAC	Common Access Card	LNP	Local Network Protection	SIP	Session Initiation Protocol
CAdmin	Cryptographic Administrator	MAC	Media Access Control	SLAAC	Stateless Address Autoconfiguration
CBC	Cipher Block Chaining	MAP	Metadata Access Point	SNMP	Simple Network Management Protocol
CCA	Call Connection Agent	MLD	Multicast Listener Discovery	SP	Special Publication
CDP	Certificate Revocation List Distribution Point	MS	Microsoft	SPD	Security Policy Database
CRL	Certificate Revocation List	MSG	Message	SPI	Security Parameter Index
CTL	Certificate Trust List	MTU	Maximum Transmission Unit	SQL	Structured Query Language
DES	Data Encryption Standard	MUX	Multiplexer	SRTCP	Secure Real-Time Transport Control Protocol
DHCP	Dynamic Host Configuration Protocol	N/A	Not Applicable	SRTP	Secure Real-Time Transport Protocol
DN	Directory Number	NAC	Network Access Controller	SS	Simple Server
DoD	Department of Defense	NAT	Network Address Translation	SSH	Secure Shell
DoS	Denial of Service	NetBIOS	Network Basic Input/Output System	SSL	Secure Socket Layer
DSCP	Differentiated Services Code Point	NFS	Network File System	STIG	Security Technical Implementation Guideline
DTM	Digital Trunk Module	NIAP	National Information Assurance Partnership	SYN	Synchronize
EAP	Extensible Authentication Protocol	NIST	National Institute of Standards and Technology	TACAS	Terminal Access Controller Access Control System
EI	End Instrument	NMS	Network Management System	TCP	Transmission Control Protocol
ESP	Encapsulating Security Payload	NTP	Network Time Protocol	TFTP	Trivial File Transfer Protocol
FTP	File Transfer Protocol	O	Optional	TLS	Transport Layer Security
FW	Firewall	OCSP	Online Certificate Status Protocol	TTLS	Tunneled Transport Layer Security
GMT	Greenwich Mean Time	OOBM	Out of Band Management	UC	Unified Capabilities
HMAC	Hash-Based Message Authentication Code	PDU	Protocol Data Unit	UCR	Unified Capabilities Requirements
HTTP	Hypertext Transfer Protocol	PKCS	Public-Key Cryptography Standard	UDP	User Datagram Protocol
HTTPS	Hypertext Transfer Protocol Secure	PKE	Public Key Enablement	ULA	Unicast Address
IAT	Information Assurance Tool	PKI	Public Key Infrastructure	UPD	User Datagram Protocol
IAW	In Accordance With	PMO	Project Management Office	UPnP	Universal Plug and Play
ICMP	Internet Control Message Protocol	R	Required	URI	Uniform Resource Identifier
IEEE	Institute of Electrical and Electronics Engineers	RADIUS	Remote Authentication Dial-in User Server/Service	v	Version
IF-MAP	Interface – Metadata Access Point			VPN	Virtual Private Network
IKE	Internet Key Exchange	RAW	Read and Write	VVoIP	Voice and Video over Internet Protocol
IPSec	Internet Protocol Security	RFC	Request for Comment	WIDS	Wireless Intrusion Detection System
IPv4	Internet Protocol version 4	RSA	Rivest Shamir Adleman		